NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A CONCEPTUAL FRAMEWORK FOR TACTICAL PRIVATE SATELLITE NETWORKS

by

Brian H. Conrad
Ioannis Tzanos

September 2008

Thesis Advisor: Alex Bordetsky
Second Reader: Rex Buddenberg

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE A Conceptual Framework for Tactical Private Satellite Networks		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Brian Conrad and Ioannis Tzanos			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The purpose of this research is three-fold. First is to examine the current state of military satellite communications and to analyze current trends in the commercial satellite communications market that support military Command and Control, as well as facilitate network operations. Second is the operational implementation of such private satellite networks within the context of Net Centric Operations, as well as within the context of a coalition environment. Third, this work will illustrate how the private satellite network could be managed, as well as understanding how the network could be used in the context of a network management control channel to exercise management of numerous dispersed network devices and nodes.

The focus will be to define, examine, and research the conceptual framework for a tactical private satellite network that facilitates Command and Control of geographically dispersed tactical units, as well as provides a mechanism for the management of tactical networks. After having acquired a clear picture of today's state and future's capabilities of SATCOM, research will be directed to how a tactical private satellite network would be implemented to support Network Centric Operations and how this tactical private satellite network could be utilized as a tool for the management of tactical networks.

During the research, a number of secondary, yet supportive topics, need to be examined, such as, how that tactical private satellite network can be implemented to facilitate collaboration between Other Government Agencies, Non-Governmental Organizations, and Coalition partners from other countries or how it would be managed to offer to its subscribers the desired service in terms of quantity (throughput) and overall quality.

To materialize the above, this thesis considers it essential to thoroughly examine a commercial base station which is fully capable of managing this satellite network under any conditions. The whole concept of this Tactical Private Satellite Network is examined based on two innovative approaches. First, the establishment of two different logical channels inside the physical one and second, the concept of a private satellite network and its implementation is examined as a method for direct delivery of data.

14. SUBJECT TERMS Remote Network Management, Satellite Communications, Tactical Network, Military Communications, Network Entry Point, Ground Control Station, Communication Gateway, Logical Channel, Direct Data Delivery.			**15. NUMBER OF PAGES** 207
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A CONCEPTUAL FRAMEWORK FOR TACTICAL PRIVATE SATELLITE NETWORKS

Brian Conrad, Major, United States Marine Corps
B.A., University of Memphis, 1994

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2008

Ioannis Tzanos. Lieutenant Commander, Hellenic Navy
B.S., Hellenic Naval Academy, Greece, Piraeus, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2009

Author: Brian Conrad

Ioannis Tzanos

Approved by: Alex Bordetsky
Thesis advisor

Rex Buddenberg
Second Reader

Tomas Housell
Chair, Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this research is three-fold. First is to examine the current state of military satellite communications and to analyze current trends in the commercial satellite communications market that support military Command and Control, as well as facilitate network operations. Second is the operational implementation of such private satellite networks within the context of Net Centric Operations, as well as within the context of a coalition environment. Third, this work will illustrate how the private satellite network could be managed, as well as understanding how the network could be used in the context of a network management control channel to exercise management of numerous dispersed network devices and nodes.

The focus will be to define, examine, and research the conceptual framework for a tactical private satellite network that facilitates Command and Control of geographically dispersed tactical units, as well as provides a mechanism for the management of tactical networks. After having acquired a clear picture of today's state and future's capabilities of SATCOM, research will be directed to how a tactical private satellite network would be implemented to support Network Centric Operations and how this tactical private satellite network could be utilized as a tool for the management of tactical networks.

During the research, a number of secondary, yet supportive topics, need to be examined, such as, how that tactical private satellite network can be implemented to facilitate collaboration between Other Government Agencies, Non-Governmental Organizations, and Coalition partners from other countries or how it would be managed to offer to its subscribers the desired service in terms of quantity (throughput) and overall quality.

To materialize the above, this thesis considers it essential to thoroughly examine a commercial base station which is fully capable of managing this satellite network under any conditions. The whole concept of this Tactical Private Satellite Network is examined based on two innovative approaches. First, the establishment of two different logical channels inside the physical one and second, the concept of a private satellite network and its implementation is examined as a method for direct delivery of data.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAL	Asynchronous Transfer Mode Application Layer
AEHF	Advanced Extremely High Frequency
AES	Advanced Encryption Standard
AOR	Area of Responsibility
ATM	Asynchronous Transfer Mode
BER	Bit Error Rates
Bn	Battalion
BPE	Business Premises Equipment
BLOS	Beyond Line of Sight
C2	Command and Control
C2PC	Command and Control Personal Computer
C4I	Command, Control, Communications, Computers and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence Surveillance and Reconnaissance
CENETIX	Center for Network Experimentation and Innovation
CEO	Chief Executive Officer
CGW	Communication Gateway
CIA	Confidentiality Integrity Availability
CJTF	Combined Joint Task Force
Co	Company
COI	Contacts of Interest
CONDOR	Command and Control On-the-Move Network Digital Over-the-Horizon Relay
COP	Common Operational Picture
COTS	Commercial off-the-Shelf
CPE	Customer Premises Equipments
CRC	Cyclic Redundancy Check
DAMA	Demand Access Multiple Access
DoD	Department of Defense
DoDI	Department of Defense Instruction

DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITCO	Defense Information Technology Contracting Office
DSL	Digital Subscriber Line
DSN	Defense Switched Network
DSCS	Defense Satellite Communication System
DTN	Disruption Tolerant Networking
EHF	Extremely High Frequency
EOIP	Everything over IP
EPLRS	Enhanced Position Location Reporting System
ERN	Emergency Response Network
Fa	Fast Ethernet
FTP	File Transfer Protocol
GEO	Geostationary Earth Orbit
GI&DS	Geospatial Information and Data Services
GIG	Global Information Grid
Gbps	Gigabits Per Second
HADR	Humanitarian Assistance/Disaster Relief
HALO	High Altitude Long Operation Network
HF	High Frequency
HG/IWU	HALO Gateway/Interworking Unit
HMMWV	High Mobility Multipurpose Wheeled Vehicle
HQ	Headquarters
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IRC	Internet Relay Chat
ISL	Inter-Satellite Links
IT	Information Technologies

JC2-V	Jump C2 Variant
JTRS	Joint Tactical Radio System
Kbps	Kilobits per second
LAN	Local Area Network
LDR	Low Data Rate
LEO	Low Earth Orbit
LOS	Line of Site
MAC	Media Access Control
Mbps	Megabits Per Second
MCTSSA	Marine Corps Tactical Systems Support Activity
MDR	Medium Data Rate
MILSATCOM	Military Satellite Communications
MIB	Management Information Base
MIO	Marine Interdiction Operations
M-SSEP	Mobile SOCOM Strategic Entry Point
MTW	Major Threat War
MUOS	Mobile User Objective System
NCO	Net Centric Operations
NCW	Net Centric Warfare
NECOS	Network Control Station
NGO	Non-Government Organizations
NIPRNET	Non-Secure Internet Protocol Routing Network
NMS	Network Management System
NOC	Network Operations Center
NPS	Naval Postgraduate School
OES	Office of Emergency Services
OFDM	Orthogonal Frequency Division Multiplexing
OGA	Other Government Agencies
OPLANS	Operation Plans
OSI	Open System Interconnections
OTH	Over-the-Horizon
OTM	On-the-Move

PBX	Private Branch Exchange
PC	Personal Computer
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PING	Packet Internet Groper
PKI	Public Key Infrastructure
PoP-V	Point of Presence Vehicle
PSTN	Public Switched Telephone Network
PVO	Private Volunteer Organizations
QoS	Quality of Service
R&D	Research and Development
RF	Radio Frequency
RFC	Requests for Comment
RMON	Remote Monitoring
RTT	Round Trip Time
SA	Situational Awareness
SATCOM	Satellite Communications
SCMAGTF	Security Cooperation Marine Air/Ground Task Force
SIE	Special Operations Forces Information Enterprise
SINCGARS	Single Channel Ground and Airborne Radio System
SIPRNET	Secure Internet Routing Protocol Network
STEP	Standard Tactical Entry Point
SHF	Super High Frequency
SMART-T	Secure Mobile Anti-jam Reliable Tactical Terminal
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Special Operations Forces
SP	Service Providers
SUV	Sport Utility Vehicle
SWAN	Support Wide Area Network
TCP	Transmission Control Protocol
TDR	Turbo Diesel Registers

TNT	Tactical Network Testbed
TOC	Tactical Operations Centers
TV	Television
UAV	Unmanned Aerial Vehicles
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UN	United Nations
UNDP	United Nations Development Program
UNESCAP	United Nations Economic and Social Commission for Asia and the Pacific
UNHCR	United Nations Refugee Agency
UNICEF	United Nations Children's' Funds
US	United States
USMC	United States Marine Corps
USSOCOM	United States Special Operations Command
VC	Virtual Channel
VCC	Virtual Channel Connection
VoIP	Voice Over IP
VP	Virtual Paths
VPC	Virtual Path Connection
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
VTC	Video Teleconference
WAN	Wide Area Network
WGS	Wideband Gap-filler System
WNW	Wideband Networking Waveform
YBI	Yerba Buena Island

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

In order to name all the contributors to the success of this project would be project in itself. Specifically, the authors would like to thank Dr. Alex Bordetsky and Mr. Rex Buddenberg for their guidance and critical feedback throughout the course of this research. We would also like to thank all the rest of the Academic Staff of the Naval Postgraduate School and especially the Department of Information Sciences for the guidance they provided and the knowledge that they imparted.

LCDR Ioannis (Yiannis) Tzanos HN would like to thank God for giving health and happiness to his family. I would like to express my love and dedicate this thesis to my beloved wife Penny and son Taso for offering me their continuous support, love and confidence throughout this tedious but joyful process. I would like also to thank my parents, Taso and Georgia, for making me what I am and for their love. Especially, to my father, who passed away few years ago, I would like to offer my gratitude for everything he has done for me. To my brother, Dimitri, I would like to express my appreciation for being a true companion on life's journey and support me, even being thousands of miles away. Last but not least, I would like to thank my thesis partner, Brian, and wish him and his family all the happiness. Your friendship, Brian, is one of the greatest gifts I have been given here.

Major Brian Conrad, U.S. Marine Corps, would like to thank God, first and foremost for bringing me on this journey and providing to me all I could ever need and want. I would like to thank Yiannis, my dear friend and collaborator on this project. I appreciate your dedication and hard work, but most of all I appreciate the friendship that has grown along with this project. I wish you, Penny, and Taso all of the best. Finally, I would like to thank dear wife Michelle for without your love and support this would not have been possible. You are my best friend and I love you dearly. For Harper and Truman; you are the sons that brighten my every day and fill each one with joy. I love you very much.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

From the moment that the famous science fiction writer, Arthur C. Clarke, first proposed in 1945 that three geostationary satellites could provide global telecommunications coverage, mankind has been enthralled by the idea of using space technology to provide long-haul communication links. Since that time, use of satellite systems has grown rapidly in various areas: Remote Sensing, Imagery, Telecommunications (Broadcast, Internet, Fixed or mobile communication services, etc.), Navigation, weather, earth observation, scientific, etc.

Throughout the years, satellite technology expanded. Today it can add truly global coverage to even the most remote areas and mobility/access to networks of almost infinite size. Constellation of satellites can solve problems for mobile terminals, such as fading, blockages, effective elevation angles, etc. In other cases, they can complement terrestrial technology, such as fibers. Moreover, satellites, because they are high above the surface of the Earth, can receive and transmit signals from huge areas: the higher they are, the greater these areas become. Last, but not least, it is often far quicker and less expensive to bring broadcasting and communications to areas lacking them using satellites than it would be to provide the same services solely by terrestrial means (Iida et al., 20).

The above capabilities highlight the major significance of satellite communications in two areas: they can bring multimedia communication services into remote areas and they can restore communication lines during major disasters. In the latter case, communications cannot rely on any prior terrestrial infrastructure because they have been entirely destroyed. Consequently, using satellite communications is something that can benefit dispersed military units that operate in hostile environments. Further, joint forces, comprised of a great variety of different participants — governmental and non-governmental — can also benefit from satellite communications

for they can operate in all kinds of emergency and disaster response scenarios. For both military and joint forces, terrestrial infrastructure is a luxury that they do not have.

Moreover, the fact that military bandwidth, through proprietary satellites, is already saturated by the routine needs or other operations of military formations, it is prudent to say that commercial bandwidth is the best alternative. The great numbers of reasons are examined in the subsequent sections of this research. Last but not least, the participants will be able to manage this network by allocating bandwidth with respect to the different situations and applications.

Generally speaking, network management is the process of controlling a complex data network so as to maximize its efficiency and productivity (qtd. in Chen et al., 1506). Managing, in terms of monitoring and controlling the network through the triad measurement-comparison-correction of the different networking devices' variables, such a multivariable network without owning the satellite asset, is a challenging task. The network manager will have to operate inside the bandwidth boundaries that the commercial service provider has assigned. He must also guarantee the robust and high quality connectivity for each participating unit. The participants must assume the satellite as transparent and must execute their tasks as if they were close to each other on a well-linked communication terrestrial chess-board. Security and identity management rules need to be implemented to guarantee that the whole network is not compromised. Data, information and knowledge need to flow undisturbed and complete to give the power to the "Edge" participants of these Net Centric Operations to best accomplish their missions. In any case, information superiority, the capability to collect, process, and disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same, will need to be assured. One of the ingredients is the robust networking.

B. PURPOSE

The purpose of this thesis is the development of a Tactical Satellite Networking concept that would allow small units to control bandwidth and use the provided satellite bandwidth for direct delivery of data and for managing the tactical networking resources.

For that purpose, this thesis proposes the term “Tactical Private Satellite Network.” The overall capability of keeping the management of such a complicated network inside the specific community of users, while the satellite services are leased from a commercial provider, is what differentiates our research from the nowadays recipes. To guarantee secure and high quality communication lines, the proposal is to keep the network management of commercial leased satellite bandwidth “in house.” The overall goal is to propose “A Conceptual Framework for a Tactical Private Satellite Network.”

Consequently, the value of this thesis is the proposal of a framework for managing a tactical network by allocating the available bandwidth to the different users with respect to their needs and the quality of their applications. The means for achieving the connectivity is the commercial leased lines — not the potentially saturated proprietary military satellite communications whose bandwidth is negotiated by the service level agreements between the provider and the consumer (military and governmental agencies). The end product will be a tactical network operating inside the overall leased bandwidths’ boundaries, but with the capability to manage this network inside them. The term that aggregates these capabilities is the Tactical Private Satellite Network.

The thesis proposes two innovative approaches:

- The establishment of two different logical channels inside the physical one, instead of an aggregated channel, which serves logically and physically both requirements. By that a portion of the bandwidth is dedicated to management data. This data is kept separate from tactical data. This multiplatform control, separation of control and data links — for generally reconfiguring the nodes or the whole networking segment of self-forming networks — has a fundamental role in tactical networks (Bordetsky and Bourakov). The proposed segregation needs to be examined, with consideration given to the impact on the operational traffic that has to traverse the same channels of the transmission media, and adjust accordingly. Overall, flexibility must exist so that, when

required, the bandwidth is limited to only the amount needed to conduct active network management when it conflicts with the propagation of real applications.

- The examination of the concept of a private satellite network and its implementation as a method for direct delivery of data. This private network will give security and availability for the provided connectivity to its subscribers. This is further enforced by the execution of network management by one or more base stations. These will be operated by the participants and not by the provider of the satellite channels.

Research for this project consists of Dr. Alex Bordetsky's online material (in the form of readings and slide presentations), extensive literature review on relative subjects, case studies or relevant scenarios (to create a roadmap of thoughts that culminates in proving the applicability of a Tactical Private Satellite Network in modern Net Centric Operations), and a series of experiments conducted to investigate the feasibility of this concept. This thesis intends to provide an overview of the many advantages that commercial satellite usage can provide to the military and other governmental operations without jeopardizing the security and quality of the communication channels. This document also aims to show that the concepts of such network management are already available, relevant, and have been used in different forms by different agencies with successful results. It is this work's contention that the primary actor who empowers such a self-sufficient network management will be one or more base stations with advanced capabilities and increased responsibilities. This primary actor will be able to guarantee that all elements of the participating units are robustly-networked. This will achieve secure and seamless connectivity and interoperability. One or more of such base stations, together with advanced sensors and well-trained users, can further achieve self-organization of such an ad hoc network.

C. SCOPE

This thesis is directed towards users who have had tactical level operational experience and have faced the problem of managing an ad hoc dynamically-formed

wireless network — or, at least, have relied on intermediary managing entities. It can also be directed towards potential candidates who could implement and examine the technical implementation of such a network. Lastly, it could be directed towards providers who could propose their candidate solutions that match the definition and capabilities of a Tactical Private Satellite Network.

This research focuses primarily on developing an understanding of commercial satellite technologies, trends, and how the military sector can benefit from them. Definition of the envisioned network, along with doctrinal specifications and case studies, are utilized to acquire a complete picture. Because the topic is broad in scope and no specific base station has yet been utilized, in-depth technical analysis of the framework is not possible; rather, an understanding of why and how needs to be investigated and, then, implemented. A series of relevant experiments with parts of that network are provided to show the merits of such an implementation. The intent is to expose readers to the basic principles and potentials of such a network.

Overall, if the major advantages of such a network can be thoroughly understood, then this conceptual framework can move to the next level. This level could deal with protocols and proposed models that will recognize the dynamic nature of such a network. This could provide strong motivation for self-forming, self-configuring, and self-healing capabilities in the network. Either by proposing the use mobile agents, specific policies or aggregated objects, the management of such a network, with complexity emerging from the different functionality of its nodes, will be challenging and crucial for the success of the operation.

D. METHODOLOGY OF RESEARCH

As we move further into the Information Age, more ways to obtain complete and secure dissemination of data and information are being introduced. Many of them are still experimental and more are conceptual. The bottom line is that information technologies (IT), with their rapidly improving capacity, quality, and cost/performance ratios, are positioned as unique resources that can enable automation, monitoring, analysis, and coordination to support the flowing of data and information from central communication

hubs to the most remote edge participants. For the purpose of this research, relevant topics that support the idea of a Tactical Private Satellite Network are identified and specific-oriented scenarios are used to prove value. Moreover, a specific series of experiments was conducted at the Marine Corps Tactical Systems Support Activity (MCTSSA), Camp Pendleton, California to confirm management feasibility of such a network. These are discussed below in more details.

1. Literature Review: Doctrinal Publications, Satellite Communications-Oriented Books and Articles

There are a great number of books and articles that support the use of satellite in creating robust and secure communication lines. Satellite technology is recognized as evolving very fast and as the only means of connecting places seamlessly where terrestrial infrastructure does not exist or is not available. Many military and civilian organizations have already converted their communication capabilities to include satellite connectivity. Many of these authors recognize that military bandwidth is becoming over-saturated; also that the only feasible, cost-effective, and practical solution is to turn to the commercial sector which already has the means (satellites) and the services (air-time) to be leased. The network management of these newly-formed communication lines is something that everybody agrees to be crucial for the viability of these networks. A query of all these academic materials was most helpful in identifying and conforming resource materials to begin building this thesis concept.

2. Case Studies and Scenarios

Different case studies are examined – with either too few or too many attributes of a tactical private satellite network in the military or in the commercial world — to illustrate their basic strengths, differences, and their compatibilities with the proposed Tactical Private Satellite Network. The network's management always remains on the side of the entity that provides the services, i.e., the military in proprietary military networks and the service provider in commercial applications.

Further, different scenarios are employed to prove how such a network management capability can help military operations (independent, joint, or international)

and humanitarian assistance/disaster relief scenarios. Each would employ Emergency Response Networks (ERNs). Common points, individual constraints, and need for effective communications are emphasized to ascertain the benefits of managing inside the total allocated bandwidth. They are formed dynamically, are mostly ad hoc and wireless networks, set their own priorities, and supervise their own desirable Quality of Service (QoS).

3. Implementation and Network Management Experiments

One of the key principles of Tactical Private Satellite Network is how the network, consisting of network devices that connect end users and satellite terminals that provide the actual transmission path, is managed as a single entity with the ultimate goal of providing robust services. It is suggested that the network, in this holistic form, can be managed from a single point within the network — specifically, that the implementation of the base station concept will facilitate the agent function in network management. Therefore, the base station would serve as the centralized agent for managing the network. The concept of remotely managing the network will be tested to provide proof that remote management is feasible and that it serves as a basis for further research and experimentation within this realm. Additionally, this work could also aid in the determination of the utilization of low-density personnel who possess critical network management and engineering skills.

To this end, an experiment is designed to test the feasibility and functionality of remote network management within the context of the Tactical Private Satellite Network. The experiment consists of a representative network consisting of network devices (switches and routers) and hosts that are connected via a commercial satellite terminal device. They are closely, yet not exactly, replicating the proposed conceptual architecture of the Tactical Private Satellite Network. Data is collected using commercially available network management software tools, utilizing the Simple Network Management Protocol (SNMP), Internet Control Management Protocol (ICMP), and a proprietary software system that is used to manage/monitor the commercial satellite terminal. The data collected aids in the development of a management concept for the Tactical Private

Satellite Network. Data of interest includes response times of networking components, the affect on the throughput of the communications link due to the introduction of management data, and the actual amount of available bandwidth consumed by the said data. Finally, a concept is proposed for managing the holistic aspects of the Tactical Private Satellite Network.

E. THESIS ORGANIZATION

Chapter I provides a broad idea of what will follow in the subsequent chapters. Its purpose is to stimulate interest — experienced or inexperienced — and to provide a baseline to specific situations that are familiar to and can benefit from the proposed network. The purpose of this chapter highlights the new concepts that are proposed for further examination and potential implementation. A roadmap is described to help the reader acquire why building a framework for a Tactical Private Satellite Network will be beneficiary for conducting modern — military or not — operations.

Chapter II is devoted to a literature review that supports the conceptual framework of implementing such a network and to further conduct network management. This is accomplished by the examination of the current state of military and commercial satellite communications and their feasibility to the application to a private satellite network. It begins with a brief illustration of Military Satellite Communications, their current capabilities, and their future capabilities. These examples will illustrate their promising future. It also speaks to their problem of oversaturated bandwidth which means that it does not completely cover military needs — routine or not. Further, commercial satellite systems' advantages are stressed to show that they are the best solution for the problem mentioned previously. A detailed subsection also examines the challenges of using commercial satellite systems for military or other non-profit and multivariable operations. Further, to make the reader familiar, or at least to remind of, the processes and the agencies responsible for the acquisition of commercial satellite services, at the behest of the military, with their strong points are shown and potential weaknesses/limitations are presented to spark discussion. The chapter provides a detailed reference to the major future trends in commercial satellite services and major leading

technologies. This further supports the claim of needing reliance on commercial satellites' services to keep up with and take advantage of the new capabilities.

Chapter III deals with the Definition and Conceptual Requirements of Private Satellite Networks. The need to introduce the theoretical capabilities is covered by a thorough definition of this network and its desirable attributes. The rationale behind the use of private tactical satellite networks is demonstrated by describing current civilian and military examples; also, the capability that is provided to users. Leaving for a little the conceptual level, Private Tactical Satellite Network design considerations are examined in terms of ultimate goals of the network designers, the logical network design, and the applicable protocols/standards relative to these networks that utilize satellites as their primary transmission means. The rest of the chapter attempts to show the significance of the Tactical Network Entry Point of this network. Either in the form of a communication gateway or a control base station, its general capabilities are stressed to highlight its significance inside the framework of managing such a challenging network. Last, a brief comparison of the existing military gateway type systems in different branches is investigated to show that even in a proprietary environment, a gateway system is the most vital piece of the terrestrial segment of a satellite network.

Chapter IV moves to the operational implementation of the Private Tactical Satellite Network in specific operational domains. It starts with the experimental domain of the Naval Postgraduate School's (NPS) Center for Network Experimentation and Innovation/Tactical Network Testbed (CENETIX/TNT) architecture and its recent implementation during Marine Interdiction Operations (MIO) 08-2. The Swe-Dish services example is used to stress the significance of a less self-dependent application and the potentials that it may have if it is fully implemented under the scope of a complete Tactical Private Satellite Network for support of future experimentation. Different scenarios of the operational implementation are built to show how this network can fit. The maritime domain, Marine Corps Security Cooperation Marine Air/Ground Task Force (SCMAGTF) case, and the coalition for military or humanitarian assistance/disaster relief operations' environments are used as "testbeds" to demonstrate the applicability of a Tactical Private Satellite Network. It is shown that proper network

management of it by participants can facilitate and optimize the results of relative operations. To summarize this chapter, a specific reference to Net Centric Warfare, or Net Centric Operations, where no force is used, show that all the modern scenarios mentioned previously belong to these broad terms. Thus, a Private Tactical Satellite Network can be a major enabling force to Net Centric Warfare.

Chapter V illustrates the testing performed on a live network and the feasibility and practicality of remote network management. A detailed treatment of the test network architecture is provided. A summary of the stated goals of testing and the rationale behind the choice of specific metrics use to collect data is included. This chapter illustrates results of testing and provides a detailed analysis pertaining to the remote management of network devices and the satellite network. Finally, specific recommendations are made to provide a conceptual model for remote network management.

Chapter VI provides a summary of the work that has been conducted and conclusions from the thesis research listed above. This final chapter provides suggestions for areas of general study and more detailed and, potentially, technical study dealing with the Tactical Private Satellite Network.

In conclusion, a specific roadmap has been built to move from definitions to operational implementations and experimental records. By that, it is believed that the reader will be able to acquire a clear picture of what a Tactical Private Satellite Network is and what challenges addresses in supporting edge operations that, more or less, include all the modern communication scenarios — military or not. It is important to understand both the challenges and the significant benefits of managing such a network to optimize the results of different operations. Before recommending how and where to implement a Tactical Private Satellite Network, feasibility and further technical implementation in different operational environments, in terms of participants and type of the operations, are amongst the aspects that need to be further addressed

II. MILITARY AND COMMERCIAL SATELLITE COMMUNICATIONS AND THEIR APPLICATION TO A PRIVATE SATELLITE NETWORK

The main role of the communication system is to ensure positive connectivity through the battlespace. This provides the ground or sea commander with the capability to effectively plan, conduct, and sustain joint military operations (U.S. Dept of Defense, Joint Publication 6-0, vii). The communications system consists of wired and wireless communications systems working in concert to provide the required capability. Satellite communications have become a necessity on the modern battlefield to provide access to modern information systems to deployed users. Even though wired and terrestrial radio systems provide greater bandwidth and overall capability, satellite systems can reach users and provide access to critical information that would support Command, Control, Communications, Computers, Intelligence Surveillance and Reconnaissance (C4ISR) functionality that wired and terrestrial radio systems cannot support due to geographic limitations.

The purpose of this chapter is to examine the operational capabilities of present military satellite communications constellations that are used to extend the Global Information Grid (GIG) to deployed users. This chapter also examines future military satellite capabilities and the capabilities of the Defense Information Systems Agency (DISA) Teleport program. An examination of commercial satellite systems in general, their economic impact, availability, and associated challenges with using them is made. The acquisition of commercial services is examined — specifically who is responsible for the acquisition of commercial satellite services and how commercial satellite services are acquired for use by the military and the Department of Defense (DoD). Finally, this chapter discusses current trends in commercial satellite systems (this can affect military use of the commercial segment) and underscores the need for the military (especially small units using their own terminals) to utilize commercially available satellite communications services to provide access to the GIG.

A. MILITARY SATELLITE COMMUNICATIONS

Military operations can occur virtually anywhere on the globe. Thus, the military must have reliable means of communication to effectively exercise command and control (C2). Due to geographically diverse and dispersed geographical areas and because military commanders are likely to operate in such areas that are lacking in mature survivable communications infrastructure, satellite communications are often the only means available of enabling beyond Line of Site (LOS) C2 (U.S. Dept of Defense, Joint Publication 3-14, D-1). Furthermore, satellite communications provide a valued point of entry into the GIG, which, in turn, provides access to information critical to the military effort. Military forces that require access to the GIG can achieve that access by two primary means. First, the military can access the GIG via terrestrial or wired communications and, second, they can access the GIG via satellite communications — either military owned and operated or via the commercial frequency bands. With both the increasing requirements for information transfer on the modern battlefield and to smaller units that have not had access to satellite services in the past, information requirements can only be addressed by the implementation of broadband communications circuits. If the communications infrastructure is not mature in the theater of operations, then military forces must rely on satellite communications systems to achieve the desired connectivity. This illustrates the importance of satellite communications in extending the GIG to tactical users. Access to the GIG via wired or terrestrial means is outside the scope of this work and will not be addressed.

1. Current Military Satellite Communications Systems and Capabilities

Because of the nature of military operations (not having direct access to the terrestrial communications infrastructure), satellite systems can be used to bridge the distance and connect forward-deployed units. These satellite systems can provide improved bandwidth capacity not normally provided by other traditional Beyond Line of Sight (BLOS) systems, such as High Frequency radio. Furthermore, satellite communications provides a valued point of entry into the Global Information Grid (GIG), which, in turn, provides access to information critical to the military effort. Bandwidth of

systems providing connectivity in the GIG environment can range from small communications pipes (a few kilobits per second (kbps)) to associated fiber networks (speeds of 10 Gigabits per second (Gbps)) (DeSimone and Tarr 2). To be more specific, according to U.S. military doctrine, the GIG includes all communications and computing systems and services, software (including applications), data, security services, and other associated services that are necessary to achieve Information Superiority that are owned and leased by the government (U.S. Dept of Defense, Joint Publication 6-0, II-1). Considered a "network of networks" the GIG is comprised of different components that are managed by different agencies, different transport mediums (fiber optic cable, satellite links, etc.), and, most importantly, requires a connection to the Internet (De Simone and Tarr 3). The GIG provides interfaces to multination and non-Department of Defense users and systems and, thus, facilitates information exchange between coalition partners and other government agencies (OGAs) and non-government agencies (NGOs) (U.S. Dept of Defense, Joint Publication 6-0, viii). To exercise successful C2 of military forces, especially those forces that are geographically dispersed, access to the GIG is a necessity and satellite communications are often the only means available to connect those units. Even though satellite communications are necessary, they do not provide the same capability as terrestrial radio or cable systems.

To provide GIG access, the military has a robust satellite communications system that takes advantage of the different characteristics provided by different segments of the frequency spectrum. Additionally, the military has procured and fielded user terminal equipment that corresponds to the portions of the frequency spectrum for satellite communications. Military satellite communications (MILSATCOM) operates predominately over three frequency bands: Ultra High Frequency (UHF), Super High Frequency (SHF), and Extremely High Frequency (EHF) (U.S. Dept of Defense, Joint Publication 3-14, D-2). The following table describes the operating frequency and the associated band designation for satellite communications systems.

Radar nomenclature		ITU nomenclature			
Radar letter designation	Frequency range	Frequency range	Band No.	Adjectival band designation	Corresponding metric designation
HF	3–30 MHz	3–30 MHz	7	High frequency (HF)	Dekametric waves
VHF	30–300 MHz	30–300 MHz	8	Very high frequency (VHF)	Metric waves
UHF	300–1000 MHz	0.3–3 GHz	9	Ultra high frequency (UHF)	Decimetric waves
L	1–2 GHz				
S	2–4 GHz				
C	4–8 GHz	3–30 GHz	10	Super high frequency (SHF)	Centimetric waves
X	8–12 GHz				
Ku	12–18 GHz				
K	18–27 GHz				
Ka	27–40 GHz	30–300 GHz	11	Extremely high frequency (EHF)	Millimetric waves
V	40–75 GHz				
W	75–110 GHz				
mm	110 –300 GHz				

Table 1. Operating Frequencies and Associated Band Designations for Satellite Communications (from http://www.ietf.org/rfc/html).

The bandwidth offered by these three segments of the frequency spectrum is directly proportional to the increase in operating frequency and, thus, provides different capabilities with different operational trade-offs for the battlefield user.

Tactical satellite systems operating in the UHF portion of the Radio Frequency (RF) spectrum support relatively low data rate secure voice and data transmission through a single dedicated channel or an on-demand assigned multiple access method to tactical users. The UHF constellation provides channels at either 5 KHz or 25 KHz and one 500 KHz channel per satellite. Due to the characteristics of the UHF satellites, the required terminals are generally small, man pack portable radios and shipboard systems, which can both be fixed or mobile, and require smaller antennas (U.S. Dept of Defense, Joint Publication 3-14, D-2). The greater beam width that characterizes the UHF narrowband satellites does not constrain the mobile users to have the pointing accuracy necessary to

make higher frequency systems work. UHF systems, due to the reduced complexity of their radio equipment, are less expensive to build and less sensitive to vibrations — conditions under which they will operate in a mobile/tactical situation. Also, satellite coverage from a single antenna is broad, meaning that the space-segment antenna does not need to precisely point at users. This increases mobility and flexibility. Earth coverage, for the UHF satellites, is achieved by multiple geostationary satellites positioned around the Earth and is depicted in Figure 1:

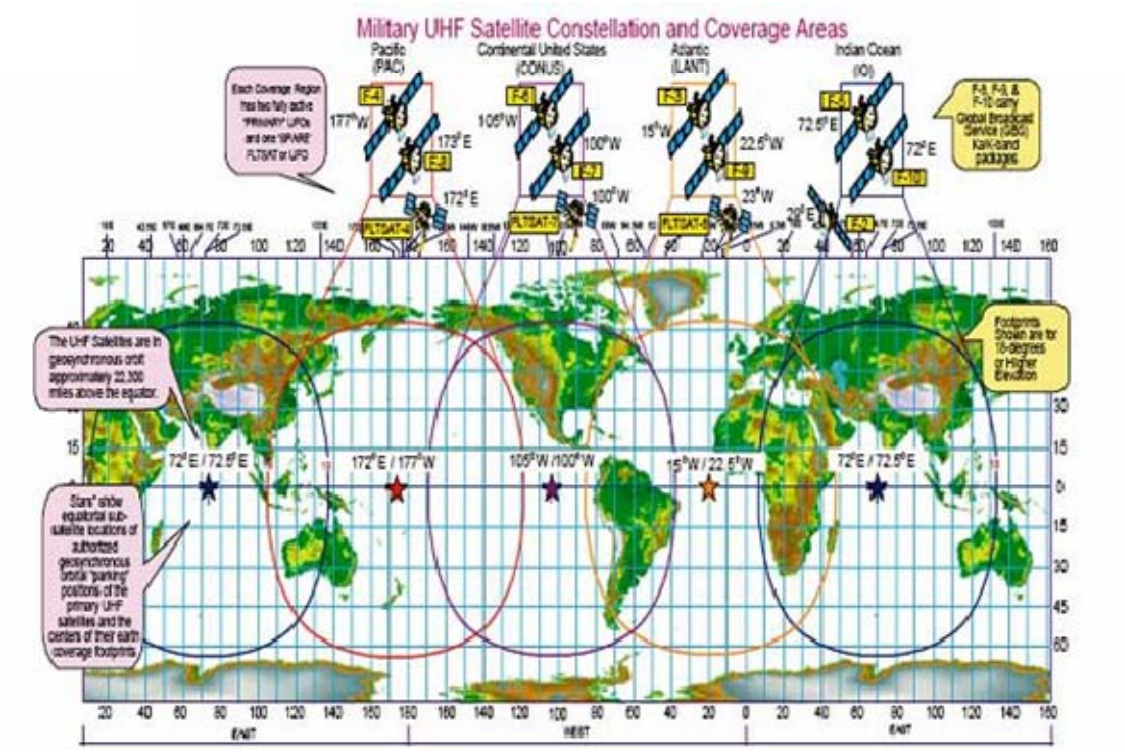

Figure 1. UHF MILSATCOM Constellation Coverage Area
(from Satellite Pointing Guide).

In addition to the UHF communications satellites, the military also operates a SHF constellation. The Defense Satellite Communication System (DSCS) is the military's SHF system. It provides wideband communications support. Wideband connectivity, according to Joint Publication 3-14, is provided by a multi-channel transmission that supports secure voice and high data rate communications for C2,

intelligence data transfer, crisis management, and high-level communications between the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the geographic combatant commanders (D-2). The DSCS satellites provide channels that range from 50 MHz to 85 MHz in bandwidth. Generally, access to Defense Information Systems Network (DISN) services, such as the Secure Internet Routing Protocol Network (SIPRNET), the Non-Secure Internet Protocol Routing Network (NIPRNET), and the Defense Switched Network (DSN) voice services, is achieved via the SHF satellites and terminals. SHF has a larger spectrum than UHF and allows for a greater throughput and, consequently, there are plenty of high-bandwidth channels available. Thus, SHF's larger bandwidth gives it higher capacity. This means it can accommodate a greater number of users on that same band. As previously noted, the characteristics of the satellite transmission directly correspond to the size of the user terminal and antenna. Thus, the fielded SHF terminals are large vehicle transportable systems with antennas that range in size from 8 meters to 16 meters for ground mobile forces. Figure 2 depicts global coverage which is achieved through multiple satellites in geostationary orbit around the Earth:

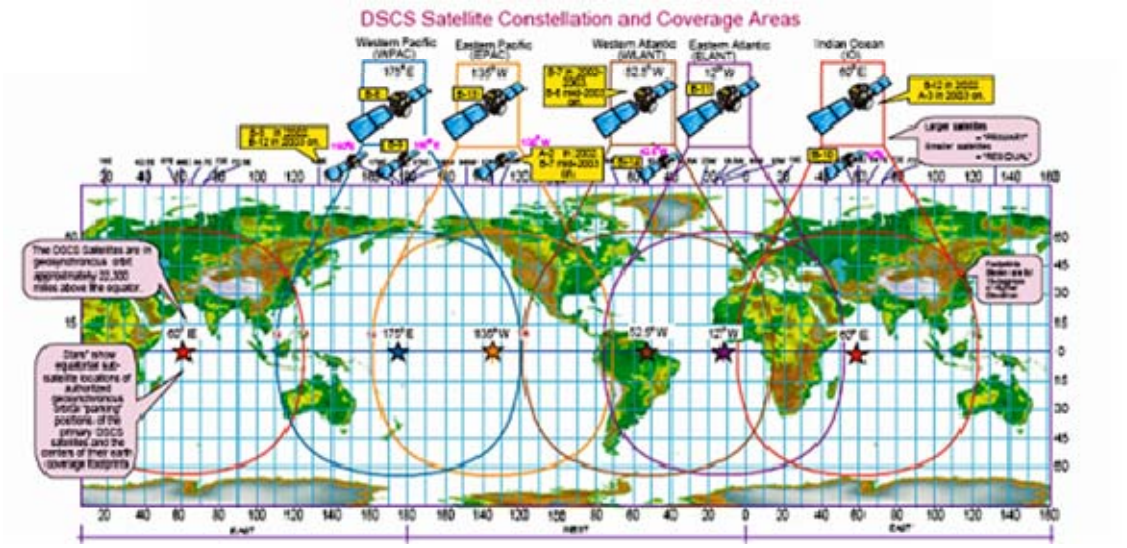

Figure 2. DSCS MILSATCOM Constellation Coverage Area (from Satellite Pointing Guide).

As noted previously, the UHF constellation supports low data rate communications and the SHF constellation supports high data rate communications. The EHF (Milstar) constellation supports low and medium data rate protected communications – survivable voice and data transmission not normally found on other systems (U.S. Dept of Defense, Joint Publication 3-14, D-2). The EHF systems allow utilizing significant bandwidth without sacrificing usable data rates for frequency hopping/anti-jam due to the very directional narrow beam that it uses. The cross link capability that these satellites have eliminates the need for ground stations, which can be a potential valuable target for adversaries' forces, and enhances the "bulletproof" significance of EHF communications. Also, equipment in the EHF range is very expensive, making it hard to exploit by other countries and, thus, decreases the number of potential adversaries. The Milstar satellites are configured to provide either a Low Data Rate (LDR) or Medium Data Rate (MDR) service. The EHF terminals are similar in size to the fielded SHF terminals and antennas. Global coverage, as with the UHF and SHF constellations, is achieved through EHF satellites and payloads that are resident on other satellites. Figure 3 depicts Earth coverage by the Milstar:

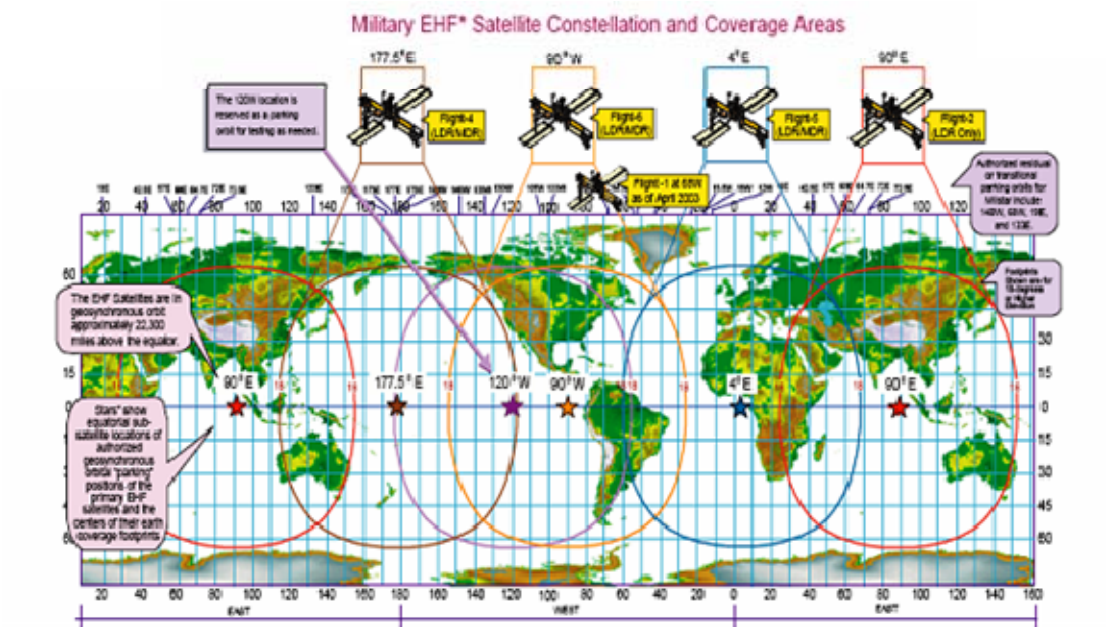

Figure 3. Milstar Constellation Coverage Area (from Satellite Pointing Guide).

2. Future Military Satellite Communications Capabilities

The existing MILSATCOM capabilities are not adequate to handle the increasing demand for wideband communications to disparate locations throughout the globe. As far back as 1997, communications planners projected that the growing demand within the military for satellite communications would exceed available military systems on a consistent basis (Rayermann 55). The only way for the military to make up the lack of capacity in military systems is to use commercial satellite communications systems. Further, there is no decrease in demand for satellite services; rather, there is a continued increase in demand. The rate of increase in the future is uncertain (Rayermann 56). DoD has realized that the current fielded MILSATCOM systems cannot handle the demand for service and access. Because of this, the DISA has transformed the Standard Tactical Entry Point (STEP) from an entry point to access DISN services via the SHF constellation (a military-only constellation) to a Teleport that provides additional capability by also taking advantage of commercial satellite bands. The commercial L-Band (500 MHz to 1500 MHz) and S-Band (2 GHz to 4 GHz) are incorporated for narrowband communications, C Band (3600 MHz to 7025 MHz), X Band (8 GHz to 12 GHz), Ku Band (10.7 GHz to 14.5 GHz), and Ka Band (17.3 GHz to 31.0 GHz). The DoD has incorporated wideband communications, too (U.S. Dept of Defense, Joint Publication 3-14, D-2). The critical feature of DISA's teleport plan is the incorporation of the additional capability (transceivers equipment and antennas) to allow commercial satellite communications to extend the GIG to military units deployed throughout the world (Rayermann 59). There are some additional advantages to allowing the military to use commercial satellite capability (these are explored in more detail in the subsequent section). The bottom line is that DoD does not have to build a great deal of infrastructure to maintain or access the commercial systems. This has advantages: reduced acquisition, operations, and maintenance costs (U.S. Dept of Defense, Joint Publication 6-0, II-10). The addition of the commercial segment to the Teleport system serves to expand the capability to connect the war fighter with critical infrastructure and information exchange capability of the GIG.

There is a demonstrated need for satellites to provide greater capability. Planners within the Department of Defense estimate that the bandwidth need to support a large joint service operation will exceed 16 Gigabits per second (Gbps) by the year 2010 (AIR WAR COLL MAXWELL AFB AL and McKinney 1). The combination of legacy MILSATCOM and commercial systems address that requirement. With the assumption that bandwidth requirements will continue to increase over time, DoD understands the need for systems that provide additional capability to support operations across the spectrum of conflict. Future MILSATCOM systems are generally classified into the following three different programs: the Mobile User Objective System (MUOS), the Wideband Gap-filler System (WGS), and the Advanced EHF (AEHF) (AIR WAR COLL MAXWELL AFB AL and McKinney 2). Each of these new systems provides additional capability over the legacy MILSATCOM systems that they are augmenting or replacing.

The MUOS system, like its UHF legacy counterpart, is aimed at the small mobile and/or man pack portable terminal with the objective of providing a higher data rate than the current UHF system (AIR WAR COLL MAXWELL AFB AL and McKinney 8). In addition to MUOS replacing the legacy UHF constellation, the legacy DSCS constellation will be replaced with the WGS constellation. The WGS constellation will supplement the current DSCS constellation with the military X-band (roughly 7–8 gigahertz), and the military Ka-band capability of the Global Broadcast Service (GBS). Moreover, the Wideband Gap-filler Satellite program will include a high-capacity two-way Ka-band capability to support mobile and tactical personnel (Elfers, Miller). The last of the legacy systems would be the EHF, replaced with the Advanced EHF (AEHF) system. The AEHF system, like the legacy EHF system will provide protected communications with about 12 times the total throughput of its legacy counterpart (AIR WAR COLL MAXWELL AFB AL and McKinney 8). Although the legacy MILSATCOM systems are very capable, the increased bandwidth requirements facilitate the need for additional systems to support military operations. These new systems, in concert with DISA's teleport program, will provide enhanced communications capability to units operating in geographically dispersed areas.

In conclusion, because connectivity to the GIG is crucial to the success of military operations, especially those in remote and undeveloped parts of the world, satellite communications plays an increasingly important role. The military has a robust satellite communications system that runs on the UHF, SHF, and the EHF frequency bands. Each of the particular bands of the MILSATCOM system provides a different and unique capability based on the bandwidth requirements of the battlefield commanders. The current demand for satellite services in the military has grown and the alternative is to address the deficiency with commercial systems. The military's bandwidth requirements will be addressed by the fielding of future systems. The use of military owned and operated constellations, in concert with commercially owned and operated systems, have increased both the ease of connecting to the GIG and the collective use for global coverage (U.S. Dept of Defense, Joint Publication 3-14, D-3).

B. COMMERCIAL SATELLITE SYSTEMS

> A strategic mix of mostly private sector telecommunications technologies and systems (leased or bought) combined with a smaller subset of DoD-unique systems integrated into a common-user DoD-wide Intranet must be the goal of the future (qtd. in AIR COMMAND AND STAFF COLL MAXWELL AFB AL and Hutchens 18).

As easily derived from the above statement of Dr. Michael S. Frankel in his February 2000 "Report of the Defense Science Board Task Force on Tactical Battlefield Communications," the concept of using commercial telecommunication systems is not new in the military environment. It is a question that has been raised after accepting that the military satellite systems cannot meet the continuously rising communication demands — especially in terms of band width, intolerable cost of research, development, deployment, and maintenance of proprietary satellite systems. This is particularly true, due to natural disasters or insufficient capabilities, where terrestrial infrastructure does not exist or is inadequate to cover the current communication needs. It is roughly estimated that the total military wideband satellite communications capacity is, optimistically, expected to grow to a maximum of 4 Gbps for the year 2010; while a very conservative estimation for the need of conducting routine and surge operations will be over 13 Gbps. This leaves a great shortfall. In predicting the additional needs for potential

Major Threat War, that shortfall in throughput climbs to more than 20 Gbps (MTW) (AIR COMMAND AND STAFF COLL MAXWELL AFB AL and Hutchens 11). Figure 4 graphically depicts projected DoD wideband requirements compared to U.S. MILSATCOM wideband capacity:

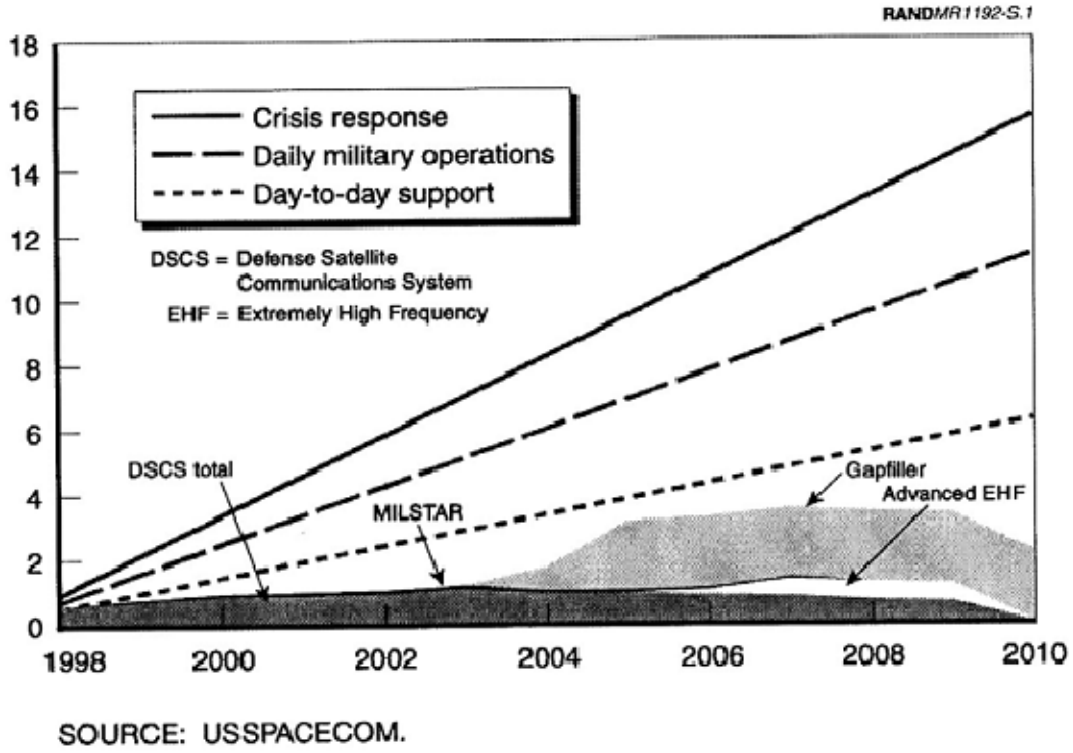

Figure 4. "Wideband DoD MILSATCOM Capacity vs. Projected Demand" (from NAVAL WAR COLL NEWPORT RI JOINT MILITARY OPERATIONS DEPT and DeMello 16).

The predicted support of commercial systems to DoD, in such a highly demanding communications environment, is depicted at Figure 5.

According to Howard Chambers, Chairman and Chief Executive Officer (CEO) of Boeing Satellite Systems, Inc:

> Another recent statistic showed that the U.S. Department of Defense currently uses 3 gigabytes per second of worldwide satellite communications (SATCOM) capacity and 80 percent of that is being provided by commercial satellites — at a cost in excess of $500 million annually. It is further predicted that the military will require 50 gigabytes per second by 2019.

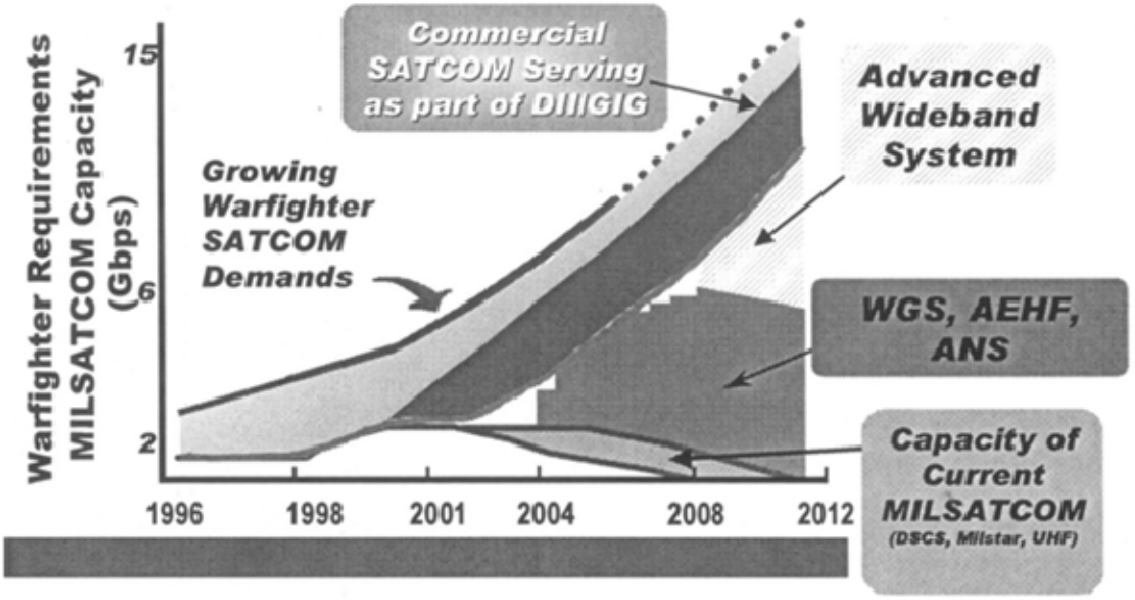

Figure 5. Commercial SATCOM Support to DoD (from NAVAL WAR COLL NEWPORT RI JOINT MILITARY OPERATIONS DEPT and DeMello 6).

Given that, it is derived that military wideband satellite communications systems cannot meet current or planned DoD requirements. It is important to note that there is sufficient commercial capacity available to meet all DoD requirements not currently serviced by organic DoD systems. Of course, the employment of commercial satellites comes with both advantages and challenges that the modern decision maker must take into account to decide if, when, and to what extent these assets can be recruited to cover MILSATCOM needs.

1. Advantages of Commercial Satellite Systems

Advantages come in both tangible and intangible beneficiary forms for the modern military environment. As in any enterprise, the tangible benefits can be measured. For the military, this includes cost effectiveness by leasing time and throughput on the commercial satellites instead of having to build or buy them. On the other hand, because military is an organization that does not measure revenues in money, it is easily recognized that the efficiency of the military operations can possibly benefit

by the use of the highly available worldwide high-capacity commercial satellites. These benefits are in communications, weather imaging, and remote sensing.

Starting from the monetary perspective, using commercial SATCOM can greatly benefit DoD in terms of economics. The costs can be reduced because no money needs to be devoted to pay for Research and Development (R&D) of new SATCOM systems. This is a major cost factor because R&D needs expensive labs with highly-skilled people to develop the systems. Also, R&D implies a significant amount of time needed for the different project phases (requirements, development, and design). DoD may not have the luxury to spare this time or money until these assets are fully operational. In addition, launching is a high-risk and expensive phase, yet the military will not have to deal with this if it will rely on commercial assets. To save all the worries that come with the pre-activation phases, the contractor will have to deliver a fully operational system to DoD.

Costs of operating and maintaining the systems do not directly affect DoD. The military has the option to pay on an "as needed" basis for the functionality and the time used. This, theoretically, saves money in the short term on paying or operating for the full functionality and time of a system. Moreover, it reduces the overhead of maintaining and upgrading a system to keep it from becoming obsolete. The latter is a constant problem nowadays with technology's fast-paced changes, but for someone who leases — not owns — a system, it is far simpler. The "customer" will only need to upgrade the contract or simply delegate the contractors to keep pace with new technology. DoD will only have to buy the needed new end-users equipment and not to maintain or upgrade the systems. Also, terminating a satellite is a responsibility of the owner. This frees military from handling this and also from the potential recovery of the satellite.

The other major, less measurable, benefit of leasing commercial systems is the time availability. Military operations can translate this availability into efficiency. The capacity that the military needs is already there: the satellites are already in orbit and the whole "hooking" can take only hours to days. Developing and launching only one satellite takes years. Satellite connections can almost be established ad hoc and on demand at every spot of the globe. This enables and facilitates military operations when time is crucial.

Lastly, the major, practical, and realistic driver for turning to Commercial SATCOM is that current and future military satellites' capacities do not suffice for the communications demands in twenty-first century. On the other hand, today's commercial satellite communications systems supply almost 1,000 Gbps of wideband capacity to commercial and governmental users worldwide. Even more growth is expected. Consequently, the need for military operations capacity is already there. Further, commercial capacity is available now to be leased and used for specific or general needs.

DoD recognizes the above advantages of commercial SATCOM. Because of SATCOM's flexibility in increasing/decreasing the level of use (measured in number of channels, transponders, or bandwidth) and in changing the distribution of resources (shift communications assets within or across geographic regions), DoD has already started to deploy them. That flexibility, in accordance with the specific leasing agreements, provides the ability to support a range of military operations across various locations/environments. Because of that, the military has come to use SATCOM in many cases as a "Gap-filler." This is leasing commercial SATCOM programs to allow DoD to keep up with its ever-expanding communications and information sharing requirements (the demand for bandwidth) more than to fill the (time) gap between fielding of successive U.S. MILSATCOM systems. In addition, when demand surges beyond day-to-day (routine) operations and operational support activities, commercial SATCOM services have been acquired to support requirements during contingency operations (Figure 6):

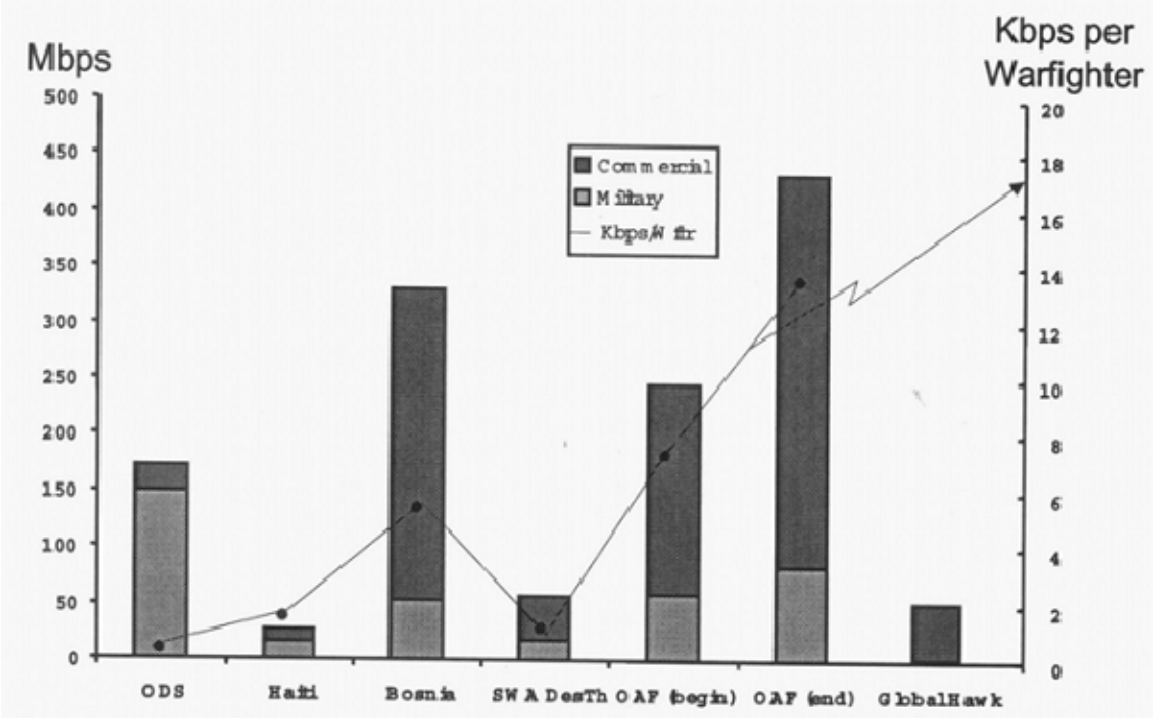

Figure 6. Commercial vs. MILSATCOM Use During Contingency Operations (from NAVAL WAR COLL NEWPORT RI JOINT MILITARY OPERATIONS DEPT and DeMello 14).

2. Challenges of Using Commercial Satellite Systems

Advantages do not come without challenges. The fact that commercial SATCOM is publicly available and wide-purposed — not military specific and proprietary — needs to be considered before planning an operation because it can jeopardize many military aspects.

At first there is no control over the requirements phase of a commercial satellite project. The military's potential specific requirements cannot be taken into account and be implemented into the design and development phase of the satellite system. Consequently, military will be treated as any other common user and will not have the ability to acquire any additional services that it may need. Further, military personnel will not be allowed direct control of the satellite. As any other customer, DoD will not have the freedom to reposition the satellite or steer its transponders to its area of interest. This

is because it will affect the usage of other customers. Hence, DoD, in general, needs to assume that it will be treated as any other customer no matter how specific or crucial its needs may be.

Security, in terms of protection of assets and data, is also a major consideration when employing commercials assets for military operations. Starting from the basic physical security of both space and terrestrial infrastructure, it can be debatable whether the contractor can provide efficient security for assets. Civilian contractors can guarantee security and redundant infrastructure for up to a level of natural disasters by deploying alternative assets, but when it comes to military operations no defensive weapons can be deployed by the company. Thus, the military may also need to provide protection for an asset which is not entirely used by troops. Further, in terms of security against soft kill mechanisms, anti-jamming defense is something entirely new for the private sector and, in many cases, does not exist to protect the quality of service that it provides.

But when it comes to authorized or sensitive data, physical security is not the only "headache" for the network administrator. As in any communication case, confidentiality, integrity, availability (CIA), and authenticity need to be guaranteed for safe and complete communication lines. This is also a major subject for commercial satellites. Confidentiality, integrity, and authenticity can be assured by the military participants by securing the data itself up to a level that NGO can be active players when needed. Availability may be doubtful because it can be guaranteed during peace time, but no one can predict how the company and its shareholders will react during a crisis period or, even worse, a war scenario. Further, the ground segments of commercial satellite networks, control stations, are run by civilian personnel who allocate the bandwidth and coordinate the efficient usage of the satellites. This raises one more question: how trustworthy and available can this network be if it is run by non-military and not certified personnel? Non-military making decisions about the operation of the satellite could affect indirectly, or directly, military or governmental communication lines.

Another characteristic of leasing assets from the free market is that DoD cannot claim a competitive advantage over its enemies. Since anyone can pay to acquire these services, it must be expected that competitors will have the same capabilities and will

know each others vulnerabilities. Under this assumption, leasing a commercial satellite system must be perceived more than a competitive response or an operational need and not as a competitive advantage that will give privileges to the military over its potential adversaries.

The major issue of interoperability must not be neglected: using commercial assets bears the danger of not being compatible with existing military or other used commercial systems. This may affect the specific parts, or even the whole operation, of the total infrastructure. Internet integration is also a major aspect of that interoperability and needs to be specifically handled to use the satellite connections up to their full potential. When the military uses Commercial off-the-shelf (COTS), compatibility and interoperability are major concerns and, thus, it is crucial when using commercial satellite networks which can be paralleled as major scaled COTS

In conclusion, commercial satellite systems comes with advantages that can be exploited, yet also challenges. If the challenges can be faced effectively, these systems could be valuable assets for the success of any military operation. It is the scheduler's responsibility to properly evaluate and mitigate the risks of using — and up to what level — commercial satellite systems in the military environment for proper, continuous, and secure military communications.

C. ACQUISITION OF COMMERCIAL SATELLITE SERVICES AND CAPACITY

Realizing that military owned and operated MILSATCOM systems do not have the requisite capability to cover the growing demand for communications services, there is a growing need to utilize commercial satellite capacity to support military operations. Commercial satellite services currently provide somewhere between 250 and 300 Gbps of wideband communications capacity to both the civilian and military markets (Mattock 1). Additionally, because the commercial satellite communications market is relatively mature, there is generally a large amount of money spent on commercial systems. For instance, in 2005, over $300 million was spent on commercial satellite communications services (U.S. Dept of Defense, Commercial Satellite Spend Analysis, 2). A critical part

of effectively leasing commercial satellite capacity is determining exactly how much commercial capacity to lease. Given the level of uncertainty for future demand, the onus is on military communications planners to determine and choose the amount of satellite communications capacity to lease that is appropriate for the mission (Mattock 1). Because there is a genuine need for commercial satellite services, the DoD set up a mechanism for the acquisition and management of contracts for commercial satellite communications services.

1. Commercial Service Acquisition

The DISA is the lead agency within DoD for the acquisition of commercial satellite bandwidth. This acquisition is done primarily through the Defense Information Technology Contracting Office (DITCO) (U.S. Government Accounting Office 4). DISA and DITCO serve as the central clearinghouse for the collection of commercial satellite requirements and the allocation of acquired resources. Generally, the process for procuring commercial communications services is fairly simple. First, users identify a need for communications services. Then, DISA technical experts aid in engineering a solution for the customer. Next, DISA contracting experts aid in the actual service procurement, determine the appropriate contract structure for the particular action, and, eventually, award the task or delivery order to the service provider (U.S. Government Accounting Office 5). Again, the issue — especially when dealing with commercial satellite services — is determining how much to acquire. It must be remembered that the U.S. military is in direct competition with other governments, civilian businesses, and organizations for the finite capacity of civilian systems. The military requires a certain amount of bandwidth on a regular basis. That is easy to predict, but what is difficult is planning for commercial services in support of established Operation Plans (OPLANS). More difficult is planning and acquiring commercial services for contingency operations. DISA, however, has an answer to this particular issue: to enable the planning for DoD's use of commercial bandwidth, recognizing that the consistency of DoD's actual requirements cannot be accurately predicted, DISA has established a layered approach to the procurement of commercial capacity (U.S. Dept of Defense, Commercial Satellite Procurement, 7). This layered approach provides an increased amount of flexibility to the

user and to the contracting agent to provide the requisite amount of commercial bandwidth to support operations. The layers, according to DoD's answer to a published GAO report, are outlined in the following table:

Layer	Required Service Level	Support
1	Long term, well defined requirements	Most stable requirements, easiest to predict, and less influenced by crisis scenarios and standing OPLANS
2	Pre-positioned capacity (Capacity in Reserve)	Requirements directly tied and related to strategic planning and oriented toward geographic theaters
3	Surge Capacity	Capacity over and above what has already been acquired and is needed to support contingency operations or other unplanned crises

Table 2. Commercial Satellite Acquisition Layered Approach (from U.S. Dept of Defense, Commercial Satellite Procurement, 7).

Through this layered approach, DISA has emplaced a robust and flexible system for procuring commercial communications services — especially commercial satellite capacity in support of planned military operations, geographic theater requirements, and capacity required to support contingencies.

2. Issues with Commercial Satellite Services

The method DISA uses to acquire commercial communications services consists of both benefits and challenges. DISA, when acquiring commercial bandwidth, does not acquire the bandwidth directly from the satellite service providers, but procures it through several competitively selected vendors. These vendors hold their own competitions between individual bandwidth service providers (U.S. Government Accounting Office 5). Therefore, through DISA's process, the government gets the most economic benefit from

the contracting effort without having to manage a competition for each contract. The ideal is to purchase/lease commercial capacity in multi-year contracts. Multi-year contracts have an added benefit of enhancing the stability and financial standing of the commercial satellite communications industry (U.S. Dept of Defense, Commercial Satellite Spend Analysis, 38). Financially viable providers will be able to continue to make their services available not only to the civilian market, but to the government and DoD as well. This continued access is also a benefit of the multi-year contracts. Generally, there are economies of scale when leasing services. Some of challenges have to do with economies of scale and long lease times. Long term leases are not at all flexible with regard to the amount of capacity that is being leased – an issue covered by DISA's layered approach discussed previously. Longer leases procured well in advance tend to be less expensive. That depends, however, on the accuracy of demand requirements. Any capacity over and above that which was procured within the confines of the long term lease must be procured through short term. This is generally more expensive (Mattock 1).

To summarize, because there is a capacity deficiency in current MILSATCOM systems, commercial satellite systems are a recognized viable alternative to augment military capability. DISA is the executive agency for the procurement and management of contracts for the procurement of commercial satellite services. The challenge associated with procuring commercial systems is in the accurate prediction of required capacity. DISA has established a layered approach to contract for commercial services based on daily operational need. This three-layer approach allows provisions for daily operational need, capacity needs oriented to capacity in reserve, and surge capacity that would be required to address the needs associated with contingency operations. This layered approach is flexible and can quickly respond to warfighter needs. Finally, there are benefits and challenges. Multi-year contracting for leased services is relatively inexpensive, but any excess capacity required can be expensive to procure and, generally, inflexible. Multi-year contracting, however, is good for the overall health and well being of the commercial satellite industry. This could ultimately ensure continued access to these commercial services.

D. FUTURE TRENDS IN COMMERCIAL SATELLITE SERVICES

Satellite technology is a relatively new area of business and has much room to evolve. Different people envision different capabilities and a vast number of new services for the satellite systems. Many of them would have seemed unrealistic a few years ago, but they have already been implemented today. It is common sense that with the exponential rate of technology's evolution, many more things will be achieved in the near future. Not all of them are related to military operations and, thus, will be omitted from the following paragraphs. Focus will be on those give direct or indirect benefit to the military. For example, the proposal of building stratospheric platforms (20 km altitude), which promises to fill an importance coverage gap (50–400 km diameter footprint at 5°-40° elevation angle), is ideal for the metropolitan footprint, but it cannot satisfy the needs of dispersed operations over a wide area. Here only the footprint of one or more satellites above Low Earth Orbit (LEO) would be covered. Therefore, in that section, this thesis refers to trends that can be exploited by the military and can be used as driving factors for the success of a military operation.

The driving force for the continuous growth of satellite capabilities is the even more growing customers' needs to use them in everyday life. While during the emergence of the satellite technologies, people were reluctant to use them either because of their high costs or the "fear" of the unknown. As the years passed, because legacy technologies could not suffice, more and more people turned to satellite technologies to achieve specific goals. These people, either as executive individual customers or as big enterprises, began to construct a robust "customer" base which, soon, took a big share of profit in significant areas of business (e.g., satellite TV). With the help of new technologies and more affordable prices, that robust customer base for satellite-delivered services has been doubling every year. It is predicted that soon everyone — at least in Western countries — will have a number of appliances with built-in satellite terminals, such as radio, TV, telephone, position location, computer, pager, PDA, etc. Figure 7 depicts earth terminals which have been used for customers' appliances throughout recent years:

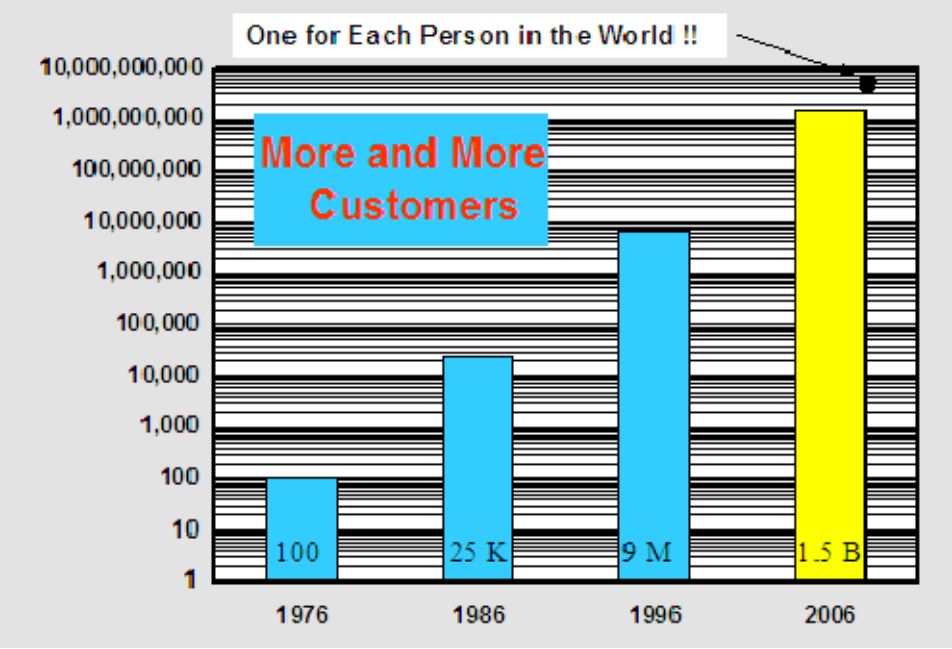

Figure 7. The Earth Terminal as Consumer Appliance
(from Hoeber, NPS Space Systems Seminar, 2000).

That growth, which is mainly driven by the high quality products and almost global coverage of satellites, gives a strong boost to the satellite R&D industry to create modern systems that meet customers' demands. To be more specific, more customers drive the need for more bandwidth availability and capacity on satellites. Satellite industry is constantly raising the bar of bandwidth and capacity to fulfill those needs. It is trying to expand this capability to every spot on the globe to achieve true global coverage. This has major advantages over terrestrial systems. Though it is too early for safe predictions, it is envisioned that the capacities of SATCOM will quickly out-pace terrestrial legacy systems.

Especially for the capacity trend, Figure 8 shows the power trend which is a crude measure of the capacity of a satellite. This figure shows how capacity has grown growing since 1976 (the same exponential growth can be traced back to 1960) and projects the trend a few years into the future. This growth may have been slow, but it is steady compared to Moore's Law for integrated circuits: "Chip performance/price ratio doubles every 18 months."

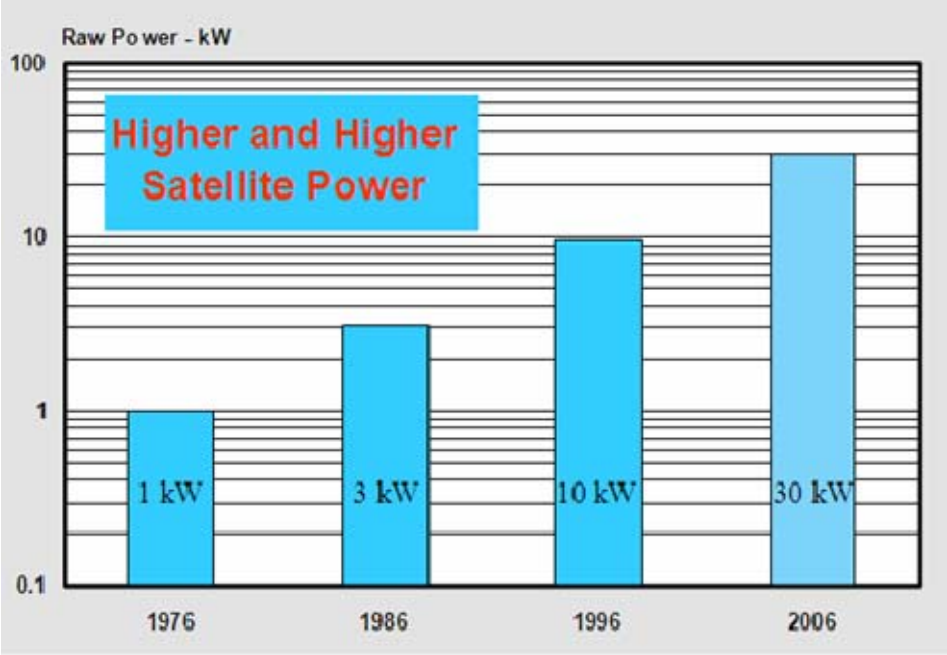

Figure 8. Satellite Power Trends (from Hoeber, NPS Space Systems Seminar, 2000).

Digging into more technical fields, the satellite companies are continuously trying to develop higher-gain and larger-aperture antennas to improve the quality of communications. Larger apertures 'pull' other satellite technologies/designs, such as flexible bodies, low thrust, energy storage, mechanisms, distributed apertures, inter-satellite Local Area Network/Wide Area Network's (LAN/WAN), and timing. Satellite companies also explore their abilities to expand available frequencies for satellite communications. This is either through spatial or other reuse techniques and/or the allocation of new and typically higher frequencies bands to avoid interferences between Geostationary Earth Orbit (GEO) satellites to face the problem of "overpopulation" in that orbital area. They are also developing patterns for building more flexible satellite antennas which are more adaptable than the previous generation. This is being accomplished using technologies that allow beam patterns to be changed on-orbit.

In terms of processing the information in orbit, the trend is to enable on board processing. This ability promises to solve significant problems of satellite communications, such as latency, waste of valuable frequency spectrum, and

improvement of overall throughput of the satellite. That overall processing is also enhanced by the arrival of multibeam satellites which enable digital processing and phased array technologies. Thus, the satellite will be able to reuse the frequency spectrum multiple times by generating many smaller circular spot beams which make possible the use of the same frequency spectrum in more than one beam.

To improve the ability of processing, two new technologies are evolving:

- Cross-Strapping allows a satellite to receive a signal up-linked in one frequency (such as the Ku-band) and retransmit it to the earth on another frequency (such as the C-band) and

- Split Up-Links enable a satellite to receive more than one up-linked signal at one time allowing multiple satellite newsgathering teams to up-link to the same satellite.

The basic space technological trends are shown in the following Figure 9:

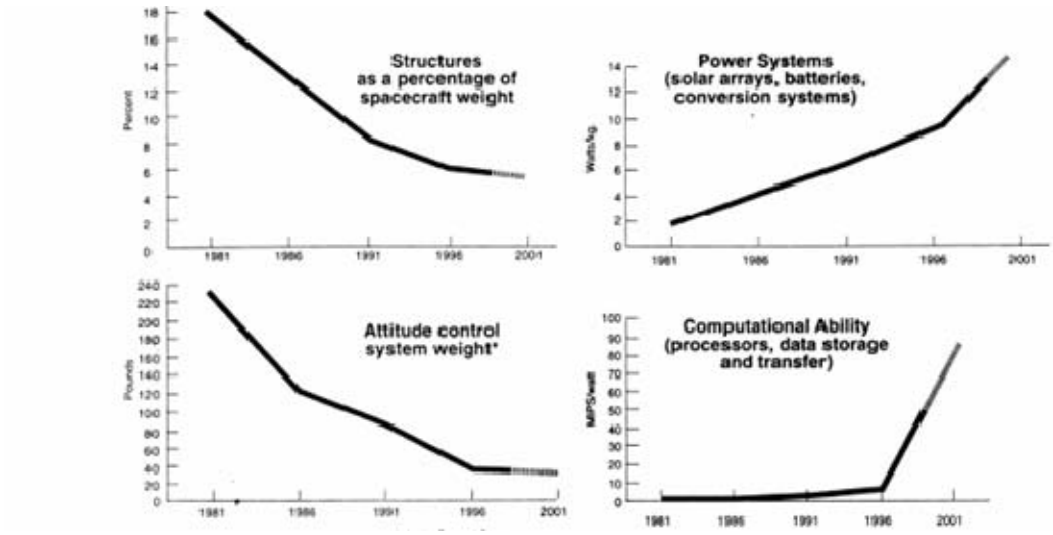

Figure 9. Basic Space Technological Trends (from Stuart).

In terms of life expectancy, the satellites' companies' main aim is to develop higher-performance, longer-lived, and larger power systems. This correlates with the target of developing products that are expected to operate for 15 years on-orbit without direct maintenance. Also, business planning for a satellite, which defines how it will be

used, is also determined for that 15-year life. This is a remarkable feat when someone considers that Long Range Business Planning seldom goes beyond 10 years and the real predictive capability is most likely 3 to 5 years — at best.

Further, to efficiently respond to the variety of demands for satellite systems and to reduce risk, satellite companies are now procuring fungible assets that can be used, sold, or leased to other business applications and customers. A decade ago satellites in orbit could perform just one specific mission. Today they can now be reprogrammed on-orbit in a matter of days. This results in increased service and capability — not to mention the profits possible with multiple-use characteristics. This is also an area that specifically involves military operations because it enables commercial satellite services to be leased for government applications by hosting specific payloads for military services. The latter is the concept of the "hosted payload." This means that commercial providers can host a payload on their satellites that can, then, be leased to the military to augment their telecommunications requirements. This is a successful technique which has already gained the attention of the satellite companies who understand the potential revenue of military leasing. Concerning the above, Chambers stated:

> This deserves attention, for today the demand for routine communications within the military — and I am referring to those that do not require encryption or other security measures — far exceeds the supply available. A recent statistic showed that the U.S. Department of Defense currently uses 3 gigabytes per second of worldwide SATCOM capacity, and 80 percent of that is being provided by commercial satellites — at a cost in excess of $500 million annually. And — it is predicted that the military will require 50 gigabytes per second by 2019.

For the space segment of satellite systems, the problem of overpopulation of specific orbits is envisioned to be handled with the development of new orbital configurations. This will combine GEO with LEO satellites as a ring constellation to purify the available orbital patterns and take advantage of the strengths of these orbital categories.

In terms of the terrestrial component of a satellite system, major improvements have entirely altered the concept of ground terminals. More and more terminals are available at reduced prices and in significantly smaller sizes. This enables installation

without — almost — space limitations. These terminals are easy to use. Depending on the purpose of deploying the system, they can be operated by average trained personnel. Overall, the increase of power combined with ease of operation, affordable prices, and other technology improvements, have allowed earth terminal size to come down much faster. They shrink by a factor of two every two to three years and the targeted customer group includes almost every household. Figure 10 depicts how the customer base has changed: In 1976, the only customers that could afford to use a satellite were a few governments. Ten years ago, large businesses could afford satellite usage. Today every household can afford some kind of satellite application.

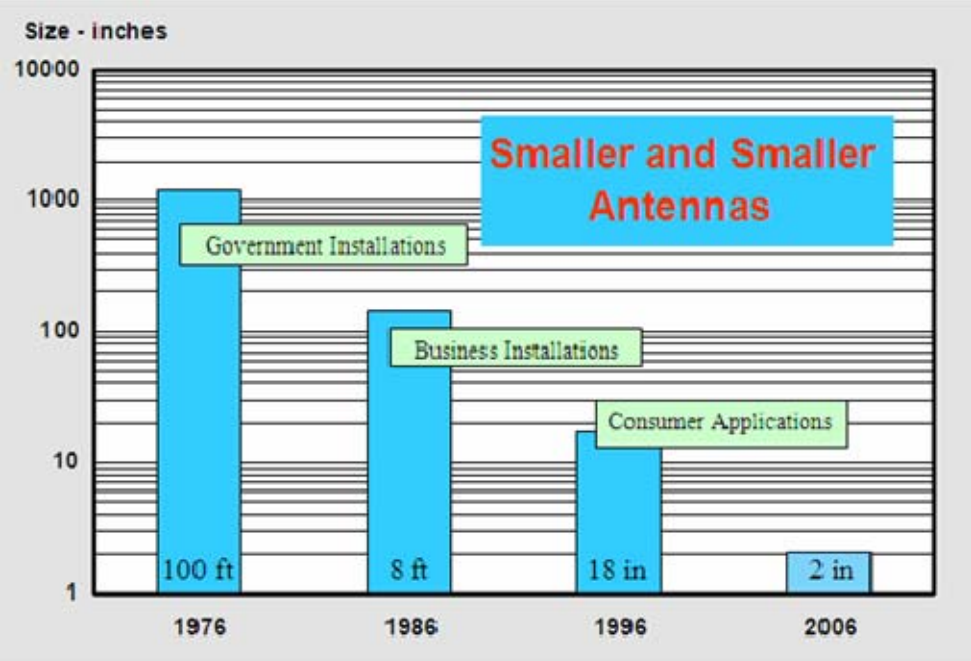

Figure 10. Earth Terminal Trends (from Hoeber, NPS Space Systems Seminar, 2000).

Table 3 summarizes some of the converging push/pull forces in the commercial space industry:

Converging Push/Pull Forces	
Business Pulls	**Technology Pushes**
- Higher bandwidths	- Power generation and storage
- Higher capacities	- Multi-beam and large antennas
- Smaller, more affordable terminals	- Deployment mechanisms
-Lower bit error rates (BERs)	- Autonomous satellite operations and operating system software
-More efficient frequency reuse and sharing	- Smart and multi-functional composite structures, flexible payloads
- Higher frequencies and powers	- Low-thrust electric propulsion
- Higher energy storage demands	Digital data processing electronics
- Larger antennas, smaller steerable beams	- Thin film electronics, batteries, etc.
- Tighter pointing (on more flexible satellites)	-Precision pointing, attitude control, timing, and navigation
- More precise station keeping	- Optical LANs and inter-satellite links
- Inter satellite links	- New frequency sharing schemes

Table 3. Converging Push/Pull Forces in the Commercial Space Industry (from Stuart).

A new but very promising concept emerging is distributed virtual satellites. The goal of this effort is to develop the technologies needed to replace a single monolithic satellite with a free-flying cluster of small satellites — each to provide a specific subsystem: communications, power, sensors, etc. The benefits from such a distribution are numerous:

- Autonomous self-forming networks.
- Wireless power systems.
- Ultra-secure intra-system wireless data communications.
- Cluster operations, such as electromagnetic formation flying systems and remote attitude determination systems.
- Distributed spacecraft computing systems.
- Structureless optical and Radio Frequency (RF) arrays.
- Reliable, robust, rapidly relocatable ground systems.

The motivation forces of distributed virtual satellites are shown in Figure 11:

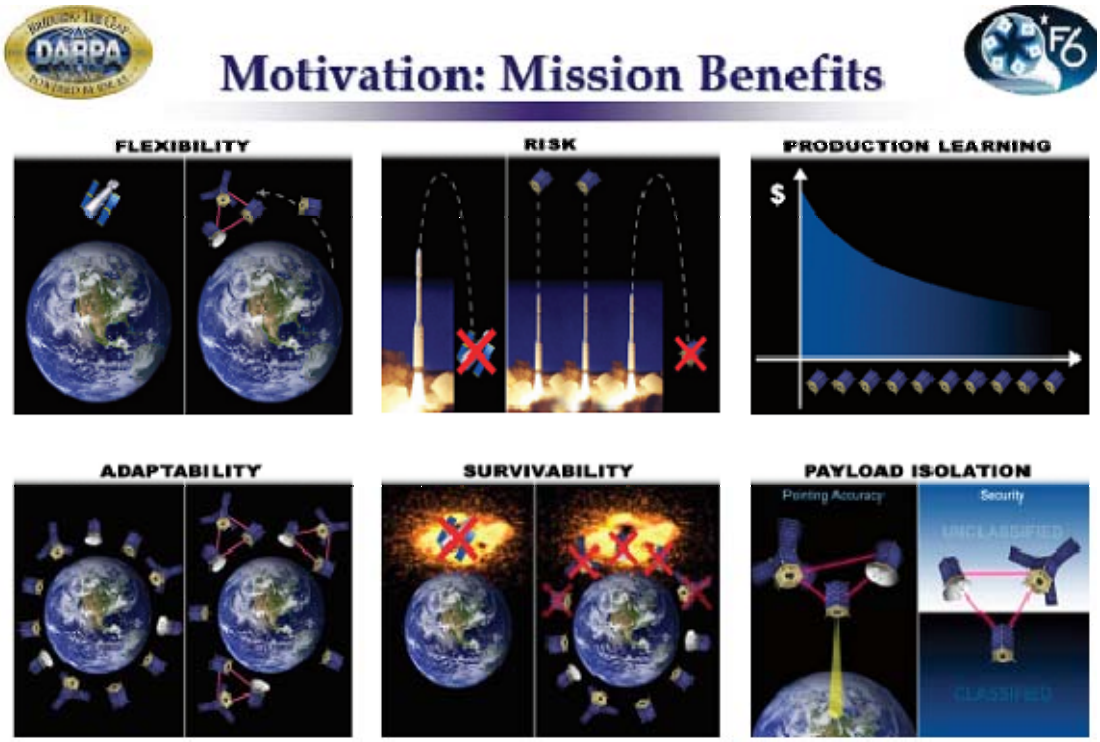

Figure 11. Motivation Forces for Distributed Virtual Satellites (from Stuart).

With regard to ground segments, we need to briefly mention that the base stations, which constitute the major focus of this research, are being continuously decreasing in size. Consequently, they no longer need to be fixed. They can be easily transported and deployed where needed. This last capability is especially valuable for the military sector when conducting operations under adverse condition; also for the government sector when executing relief operations for humanitarian purposes during or after major natural disasters. In situations that lack the luxury of time or large available sites, flexible and volatile systems, which can be easily and quickly established, are needed to achieve successful mission.

The commercial satellite industries have begun to recognize the need to protect their assets to guarantee the availability and quality of services for their customers. This aspect is specifically interesting for the military operations: the need is for high levels of assurance. This trend deals with anti-jamming techniques. These are increasingly

discussed among commercial operators as incidences of signal piracy and signal jamming — and lost revenues associated with them — rise. That also did not escape the attention of Howard Chambers' keynote speech during the Boeing luncheon in France, Paris, on 2007. "In this highly competitive industry where continuous communications — 24/7 — is an imperative — satellite providers must be able to rely on not only the quality of their signal, but the integrity of their signal."

Concerning the satellite industry, no matter how many new domestic and regional entities have emerged, the dominant trend is a move toward global integration or, at least, strategic partnerships. This globalization tendency intends to add flexibility because, as in any industrial sector, merging companies accumulate more capital investments and enhance their overall capabilities. Conversely, rather than the military dealing with a single company of trusted nationality, but with a board of different investors of different countries — friendly or not. This could potentially jeopardize the security and success of military operations. For example, the company Sea-Launch has its homeport in Long Beach, California, but it is a partnership of five companies from three different countries (USA, Norway, and Russia).

In conclusion, the overall trends of satellite industry aim not only to compete with the terrestrial communication, but to integrate with them to complete each other to achieve the best communication coverage around the globe. In most cases, this interoperability is a necessity. Thus, mobile satellite services can work together with the ancillary terrestrial components of the same network. By continuously improving the performance of the satellite systems, the trend is not to completely replace the existing terrestrial infrastructure, but to further improve the total level of communication among human beings. This is particularly true if we begin to think about the potentials that satellite systems can provide in the case of long-term habitation in space (Iida et al., 195-96).

E. CONCLUSION

> In the early 21st century, two levels of satellite telecommunications appear to be emerging. A limited capacity, owned and operated by the military, will continue to service the need for highly protected and assured

> connectivity. The continued evolution and possible integration of legacy systems should fill this need. However, an increasing percentage of operational throughput and secure telecommunications needs will likely be provided by commercial or commercial-based USG owned or leased systems. As the commercial marketplace is increasingly driven to provide secure, tamper-resistant and interoperable capacity to meet the demands of the national and international marketplace, the military will soon recognize the opportunity to conduct information exchange with significantly fewer and less complex organic resources (qtd. in AIR WAR COLL MAXWELL AFB AL and Hook 38).

By reading these words of Major General (USAF, Ret.), William G. Jones in his "*White Paper on Space in the USAF,*" it is easily understood that the military has already perceived the value of commercial satellite systems and relied on many of the capabilities provided by the commercial space sector to achieve mission success. Based on future projections, the military will never have the resources or the requirement to provide the most robust capabilities available in MILSATCOM systems to its numerous users. Thus, DoD will always require commercial SATCOM systems to augment capacity. Commercial SATCOM can be expected to meet, at least, military "gap-filler" requirements in terms of availability, but with extra care in flexibility, access, and control factors. The best approach is to view commercial space and military space as complementary in a mutual partnership for the common interest. Whether the military's growing dependence on these commercial SATCOM systems is strength or vulnerability will be determined by how well the "right mix" is achieved. Determining that right mix is a function of clearly understanding both DoD's requirements and the vulnerabilities and risks associated with a dependence on commercial systems. Basically, it would appear that commercial capabilities can help satisfy quantitative requirements, but at a "cost" in many cases of accepting risk with respect to the qualitative requirements. The decision maker will need to determine the most efficient and effective employment of commercial SATCOM — whether it be for routine day-to-day communications or leveraged to meet contingency operations requirements.

Concerning the specific feasibility of a private satellite network, satellite companies have been using them in small and large scales since the beginning of SATCOM. The use of such a network for military operations comes almost with the same

advantages and difficulties as leasing an individual satellite capability. The strong point of such an implementation is that the military will be able to operate the critical ground control station without having to rely on civilian unauthorized personnel. The only commercial owned assets will be the space ones, the satellites, for which the contractor will have to guarantee their proper operation.

By closely examining the above, it is almost indisputable that any military policy needs to facilitate further dependence on commercial SATCOM and more Commercial Geospatial Information and Data Services (GI&DS) capabilities wherever practical to meet military operational and national intelligence requirements. Commercial GI&DS are continuously improving timeliness and availability. This enhances operational utility to the combatant commander. When next-generation higher capacity and earth imaging systems come on-line and with an improved ability to deliver its products to the battlespace, commercial SATCOM and GI&DS can be expected to fill an even larger operational niche throughout the period.

Consequently, space force enhancement will continue to benefit from the growing field of commercial space applications. It is paramount that the military identify space system requirements to properly decide on the correct qualitative and quantitative use of commercial SATCOM. This will provide the combatant commander with a robust "operational toolbox" from which to obtain and maintain information superiority across the battlespace. Furthermore, combatant commanders must identify their space force enhancement requirements to ensure that the decision makers accurately assess nation's future need for commercial space capability.

To conclude, after the above brief examination of the current state of military and commercial satellite communications, it is reasonable to articulate that they have a lot in common. With both their strengths, the military's concern with security and the commercial's rapid adoption of new technologies to become more competitive than other providers, there is much benefit for both parties. The main thing that makes commercial systems more attractive is their capability of providing all the bandwidth that the military needs in any type of operation that cannot be covered by military's proprietary systems. This obvious availability of commercial "state of the art" satellite technology justifies

their feasibility for application to a Tactical Private satellite network for the military and other governmental purposes. This is not a new concept. Rather, DoD already employs it via its MILSATCOM systems. It can be further expanded, however, in areas and cases which exceed the capacity and flexibility of the military private networks. Consequently, those private systems are freed to be used for other types of operations which demand specialty.

III. CONCEPTUAL CAPABILITIES AND DESIRED REQUIREMENTS FOR THE TACTICAL NETWORK ENTRY POINT

A. TECHNICAL DEFINITION OF TACTICAL PRIVATE SATELLITE NETWORK

To examine the concept of a Tactical Private Satellite Network requires clearly defining what that network will be, determining what the functions will demonstrate, and identifying who will participate. The initial approach to determine what this network should cover originated from trying to recognize and incorporate into a network these specific attributes. Thus, this thesis attempts to dissociate the sub-definitions of such a network (Private, Tactical, and Satellite) and, then, to integrate their characteristics in an accumulative network entity:

- Private Network: A private network should provide routable Internet services to a specific and authorized set of users (different from a public network which provides services to the general public). Its subscribers do not need to login or subscribe, but they are automatically "embodied" into the network as soon as they are connected to it. This network must be "open" to allow for various users (Joint and Coalition partners, Non-Governmental Organizations, and Other Governmental Organizations) to join the network and to create an ad hoc joint/coalition network. Proper Identity Management rules should apply to allow such a variety of participants. There should be no neglect of the use of secrecy mechanisms (confidentiality) in specific parts of it or isolate "identity management silos" without strong justification. Operating via private hubs and deployable military owned and operated ground (base) control stations gives the administrator full authority over the network. This allows access and determines QoS attributes — essentially executing management

functions using bandwidth provided by the satellite network. Overall, the administrator should not have to rely on shared public networks prone to malfunction and operating failure.

- Tactical Network: Such a network must serve tactical needs and it will be primarily utilized for the duration of the specific mission (tactical span). Tactical networks include not only networks used for Command and Control of military operations, but also for ERNs. The latter are utilized during relief operations and are rapidly assembled to respond to ad hoc crises. This is where delays translate directly into death, disease, and other significant lost opportunities. To cover the needs of military, or other significant missions, the network needs to be a mobile ad hoc network. Due to the way of forming and operating, the suggested topology would be a point-to-point or a mesh. It should not prohibit a flexible star topology. This is where many nodes are directly interconnected to provide multiple routes for data to follow between two points. This achieves high fault-tolerance which essentially provides a broadcast, unicast, or multicast capability. Due the tactical nature of such a network, user type ranges from individual operators, and their sensors, to whole military formations or divisions.

- Satellite Network: This is the broad term for a network using radio frequencies relayed by satellite. It contains space segments (satellites) on which it relies for the propagation of radio frequencies and, in many cases for the processing of the transmitted data. There are also terrestrial segments which involve transmitters, receivers, and base stations which manage the communication lines. It can be integrated with other terrestrial (wired and wireless) means of communication for redundancy or smooth migration, but the main transmission operation is accomplished through satellite assets. The desired goal is the true global coverage. This can be accomplished by the integration of the satellite segment with mobile and flexible ground stations for the terrestrial segment. The

> network requires an entry point, or gateway, that acts as the controlling entity for access to Transmission Control Protocol/Internet Protocol (TCP/IP) Internet services. The entry point will have two logical entry points: one for traffic related to Command and Control and one entry point for network management functionality. Further, satellite communication aims to provide greater security and higher reliability than radio systems, public networks, and Internet solutions. So far satellite networks have demonstrated that they are less prone to unauthorized access (hacking), virus infections, and disruption in service due to public works.

In conclusion, rather than being framed by a simple definition, a Tactical Private satellite network must incorporate all the above attributes to guarantee safe and reliable ways of communication for its users. The type of expected missions are highly demanding and, possibly, under unpredictable environmental conditions and without the luxury of relying on the traditional terrestrial infrastructure. Consequently, that network must be structured to be the undisputable solution for highly-reliable communication worldwide. It should also be independent of any needed prior built terrestrial infrastructure for any of its sub-operations, such as transmission, reception, or management.

1. Rationale behind the Use of Tactical Private Satellite Networks

In both civilian and military applications, there is an increasing number of emerging private satellite networks. A number of them tend to be longer lasting to cover routine and permanent needs of the responsible organization for a specific area. They have the luxury of proper scheduling and project management. Others tend to be more “tactical” and are formed for specific missions and time duration due to the nature of the assigned tasks. The latter finds more paradigms in civilian non-profit organizations and military commands where the benefits are less tangible and are based on how fast the network will be formed — not on its pre-existence.

For example, civilian profitable companies have private satellite networks for telephone or TV services which depend on the robustness and permanency of their operation. Such networks are not expected to deal with situations other than the designated ones and cover specific pre-decided areas. Governmental organizations also work with such networks to assist in the dissemination of information for various agencies, such as air traffic controllers or connections with public buildings which lack the proper terrestrial infrastructure.

On the other hand, there are many cases where Tactical Private satellite networks need to be formed to deal with unexpected situations in non-scheduled areas and under adverse conditions. Such networks can be deployed by governmental organizations to assist various civil agencies (Highway Patrol, Fire Departments, Department of Transportation, Relief Agencies, Police, and various other law enforcement agencies) in case of crises. Special cases of the above are the humanitarian relief operations where the participants cannot be easily predefined. They can contain governmental organizations, NGO, and military units which all work together for the common good. They must cooperate and coordinate their actions to accomplish their common targets. This kind of Tactical Private Satellite Network needs to be flexible enough so even small units will have the ability to deploy and administer it.

Typical examples of Tactical Private satellite networks can be found in the military environment for the sake of “pure” military missions. The deployed units operate in hostile territories far enough from their bases and without the proper terrestrial communication infrastructure. These units need to be real-time connected with their headquarters to be recipients and senders of all the available information. They must form a clear tactical picture for their area of operations. This is particularly true today, that we live in the era of Net Centric Operations and we advocate terms as “Power to Edge” where continuous and uninterrupted communication is needed so as these operations to be executed and “Power” to be handed to the “Edge.”

In the next subsections, a number of civilian and military Tactical Private satellite networks will be briefly described to show the rationale behind the use of those networks and the fundamental benefits that their proper implementation brings to their "subscribers."

a. Civilian Examples

As mentioned above, there is a great variety of private satellite networks in the civilian world. They can either be categorized as tactical, capable of responding in crises' situations, or as "permanent" on which enterprises base their business continuity strategies. They can be further identified as independent networks which operate on main roles or as redundant networks ready to take over in case of major disaster in the primary terrestrial network. The latter constitutes the concept of the hybrid network which can be seen as an overlay of a satellite network layer and a terrestrial network layer. In these hybrid networks, satellite networks complement the primary terrestrial solutions by providing back up capabilities and making the whole network "fail safe." This keeps the most important — if not all — customer applications alive in a failure situation.

A good example of the diversity and ongoing potential of the private satellite networks is the pilot program of the "HALO Network" (Colella, Martin, and Akyildiz, p.142-148). Figure 12 shows the system architecture of the HALO Network:

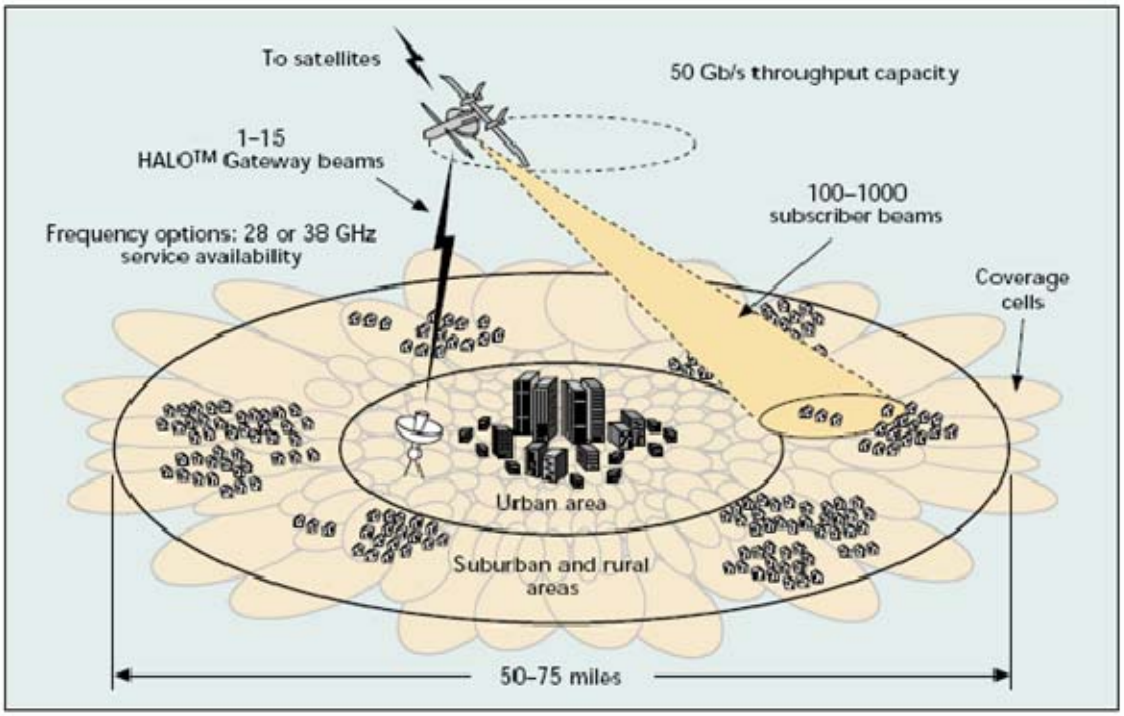

Figure 12. The System Architecture of the HALO Network.

"HALO Network" differs from the well-known "traditional" TV and phone satellite networks because it is not based on LEO or higher constellations. The High Altitude Long Operation Network (HALO) is a broadband wireless metropolitan area network with star topology. Its solitary hub is located in the atmosphere above the service area at an altitude higher than commercial airline traffic. That hub is the HALO/Proteus airplane which is the central node of this network.

That concept of HALO Network envisions combining the advantages and minimizing the disadvantages of both the satellite and terrestrial wireless networks. Such a stratospheric network, while it will offer quasi free-space channels due to clear line-of-sight signal paths offered by high look angles, will not have the "satellite overhead" of expensive high-power user terminals, long propagation delays, and stagnant performance growth. Also, system capacity will be practically fixed and can be increased incrementally only by adding satellites. It will offer the advantages of a terrestrial network, such as low-cost, low-power user terminals, short propagation delays, and good scalability of system capacity. It will be free of "terrestrial problems," such as low look

angles, multipath channels with Rayleigh fading, complex infrastructures, base stations that must be interlinked over cables or microwave links to backhaul aggregated traffic, and the often required significant reengineering to increase capacity when using cell-splitting technique. The signal footprint of the network, its "Cone of Commerce," will have a diameter on the scale of 100 km which covers a typical large city and its neighboring towns. The initial capacity of the network will be on the scale of 10 Gbps with growth beyond 100 Gbps. The network will serve the communications needs of each subscriber with bit rates in the multimegabit per second range.

That kind of network will require four types of network elements to be connected directly to the onboard switch for the proper operation and connectivity in the covered area:

- The Customer premises equipments (CPE) which are low-rate user terminals and they will satisfy the needs of individual users,
- The Business premises equipment (BPE) which are high-rate user terminals and they will satisfy the needs of specific group of users with, normally, additional included local networks,
- The HALO gateway/interworking unit (HG/IWU) which will be the equipment that provides the portal and interfaces between HALO and non-HALO networks, such as Internet and frame relay services which must be connected to the public ATM networks before they are connected to the HG/IWU, and
- The Network control station which is responsible for the maintenance, operation, and administration of HALO Networks.

Overall, there a great number of accommodated designed objectives of such a private satellite network which will provide wireless broadband communication services. Some of them deal directly with the aspects of a Tactical Private Satellite Network while others deal with the aspect of having a permanent satellite network over a subscriber's area. Among them, the most significant ones that make it a good civilian paradigm are:

- Seamless ubiquitous multimedia services.
- Adaptation to end user environments.
- Rapidly deployable to sites of opportunity.
- Bandwidth on demand for efficient use of available spectrum.
- Network Control Station with full “authority” over the management of the network.

A drawback of HALO Network, which does not diminish its value, is the relatively small area, which makes it inappropriate for disbursed military operations. This is due to the low flight altitude of the satellite asset, in this example, the HALO/Proteus airplane. It guarantees all the above mentioned advantages, but restricts the coverage area in the footprint of a metropolitan area. Nevertheless, by having the ability to manage the HALO Network as needed, the potential of the benefited enterprises are maximized — especially in regions where the existing infrastructure is not amenable to an upgrade or retrofit.

Another good example of a private satellite network is the “HughesNet Access Continuity” service which is an automatic failover network that eliminates downtime and results in considerable savings for the regional car dealership (“HUGHESNET ACCESS CONTINUITY BRINGS ROUNTREE AUTOMOTIVE’S IT STAFF PEACE OF MIND,” 34-35). Figure 13 depicts the T1 circuit with satellite failover HughesNet Access Continuity:

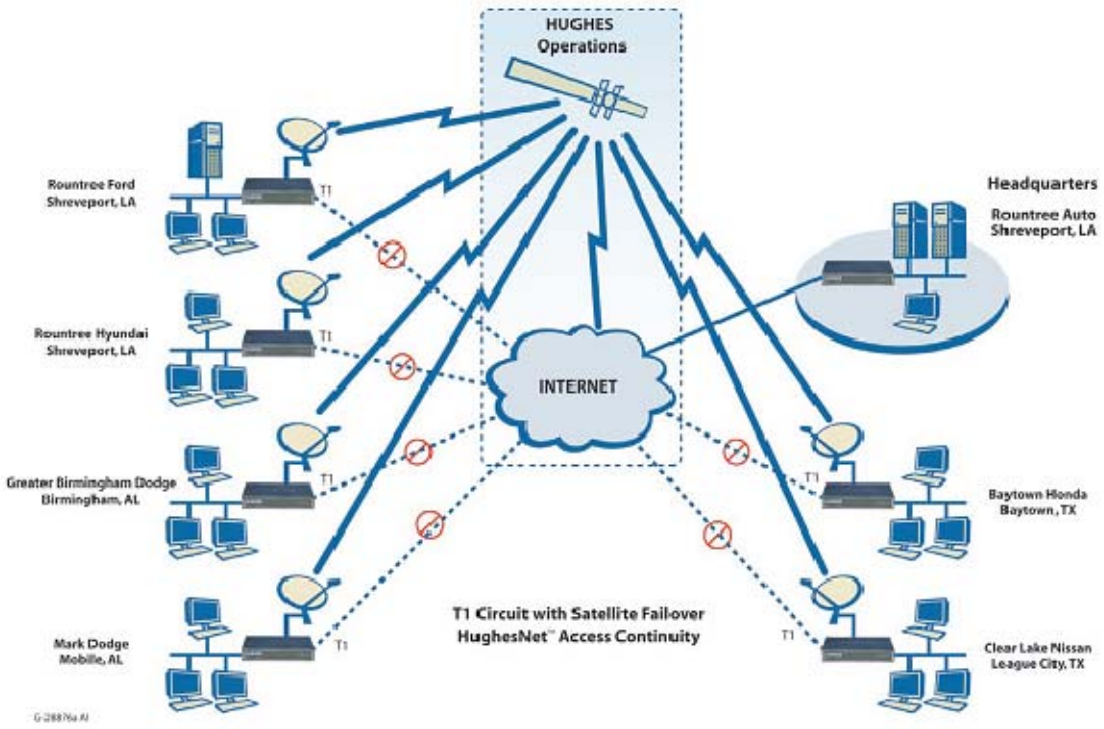

Figure 13. T1 Circuit with Satellite Failover HughesNet Access Continuity.

The whole concept behind the above private satellite network is that it provides Rountree Automotive with automatic failover to a broadband satellite connection. In the event of primary landline failure, it is delivered over their entire multi-location landline network. That network bases its function on the easy-to-use HughesNet Customer Gateway portal. With this business owners can monitor and "manage" their sites in real-time from anywhere they have an Internet connection — anywhere in the world. That gateway is the part of the overall service that monitors the customer's primary landline Internet connection (DSL, cable, or T1) and automatically switches over to a backup broadband satellite Internet connection in the event of failure. In addition to satellite backup, the appliance enables the small business to take advantage of a comprehensive list of much needed security services, such as site-to-site Virtual Private Networks (VPNs). This translates into securely connecting distributed offices over the Internet, industrial strength firewall, and potent gateway antivirus security to keep unwanted traffic and malware from corrupting their networks. Another advantage is that

the HughesNet service can be installed in a new store even if terrestrial broadband is not available in that geographic area. When a T1 solution becomes available, the store switches to that as its link with satellite as a backup.

The overall management of that network is executed mainly by a designated Hughes support team. This team acts as a helpdesk and desktop field services' team. They manage the network for the best of their customer needs and provide secure remote access and content filtering to ensure customers' employees are not wasting valuable business time on personal usage. The basic management function that is left to the business owners (customer) is the freedom to add more stores to the network. This was something businesses once considered a costly undertaking because, to add more stores, they had to add more costly phone lines to support the terrestrial network. As already mentioned, that it is not the case anymore. The whole management function is completed with the Automotive automatic failover.

The above network falls under the category of hybrid networks which can be seen as an overlay of a satellite network layer and a terrestrial network layer. They can operate on main roles or as redundant networks ready to take over in case of disaster in the primary terrestrial network that prohibits it from properly operating. Those networks are a major trend and match the concept of the satellite industry. This aims not only to compete with the terrestrial communication means, but to also integrate with them to complete each other to achieve the best communication coverage around the globe. It is a private satellite network, but the user has limited management authority. There is also a "tactical" aspect to such private satellite networks, such as the Hughes where new subscribers (new stores) can be added on demand. This eliminates the drawback of not having legacy infrastructure and the delay of constructing one.

Finally, an excellent representative paradigm of a Tactical Private Satellite network is considered to be the Kromos-Anacom network. It has been chosen by the State of California Office of Emergency Services (OES) to assist the various civil agencies in crises of natural origin. This considers that California is prone to earthquakes,

landslides, flash flooding, contamination due to hazardous materials, forest fires, and emergencies due to terrorism (Chandran, 17-18). The system configuration of Kromos-Anacom network is shown in Figure 14:

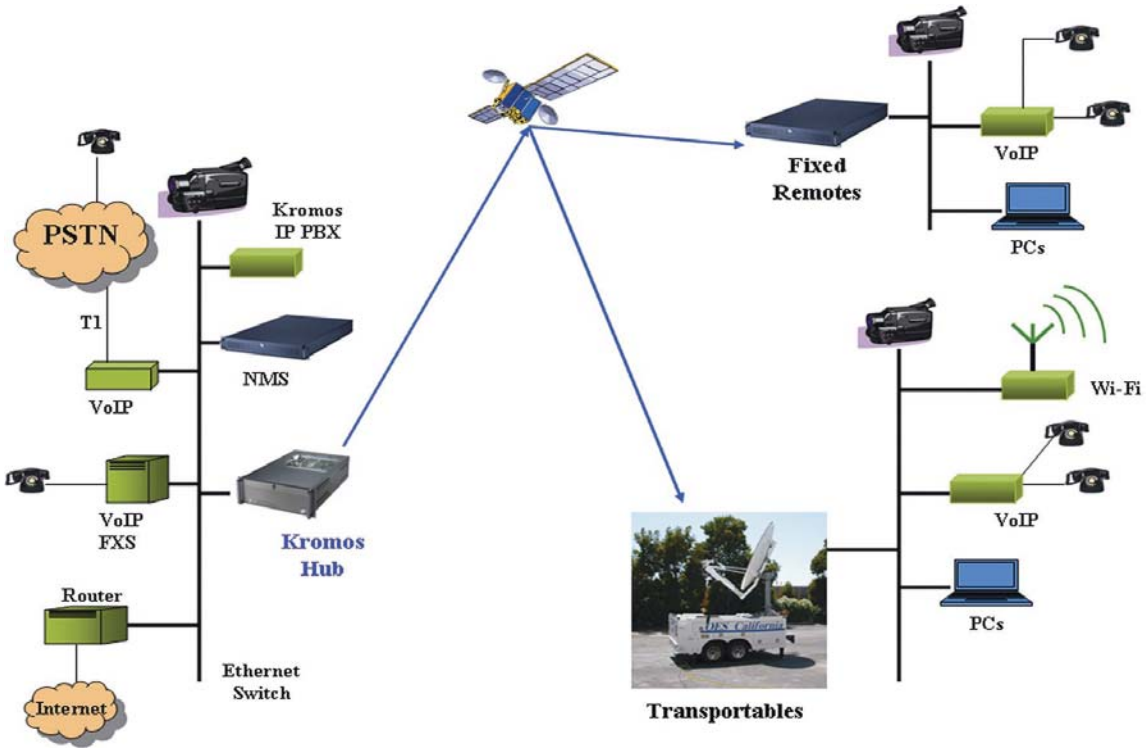

Figure 14. System Configuration of Kromos-Anacom Network.

The concept behind the choice of the above configuration-solution was that OES was looking for a modern communication network for emergency responses. It was clear that, under those adverse conditions for any kind of terrestrial infrastructure, a satellite-based solution was the only alternative to provide first responders with:

- Quick deployment of system at the sites of incident.
- Restoration of communication (voice, data, and video) anywhere in the state.
- Interoperability with the existing Infrastructure.
- Easy installation, operation, and maintenance.
- Cost competitive.

In addition to meeting its mentioned basic requirements, the final choice was also based on flexibility, scalability, bandwidth efficiency, advanced Voice over IP (VoIP), and sophisticated Network Management System (NMS) that the above network provides the users.

The above network is comprised of the following three basic elements that contribute to its flexibility and quick implementation under the crises conditions:

i. The Hub is the "heart and mind" of that network and deployed at the OES Headquarters. For managing the network and connecting with the different sites, the hub has an NMS platform, a VoIP Gateway, IP private branch exchange (PBX), and connection to the phone company (PSTN) through a T1 line. For communicating with the satellite, it uses a high power Anacom Transceiver and a large dish. The whole facility also has generators for back-up power. A significant factor of that configuration, ensuring uninterrupted operation of the network in case of an emergency, is that there is a redundant Hub installed at a separate location. This redundant Hub will assume the role of the primary Hub in case the primary fails or is rendered ineffective due to an act of terrorism or other crises. Further, the above configuration does not require the redundant Hub to be connected to the primary Hub using a terrestrial link.

ii. The Fixed Earth Stations are the majority of remotes. Each of these sites has a Kromos Satellite IP Gateway, a VoIP Gateway, and PCs connected using an Ethernet switch. Some of them have a video conferencing facility. Their outdoor equipment consists of an Anacom transceiver and a small dish. To gain flexibility and reduce delays, most of the remotes talk to each other through the Hub (STAR Topology); some of the "high-priority" remotes are enabled to connect to each other directly in a single hop (Mesh Topology).

iii. The Transportable Stations are the dynamically deployed stations of this Tactical Private Satellite network. These stations are typically mounted on trailers that can be towed using a truck or SUV to any site that requires immediate voice/video/data connectivity. Some of these stations are also vehicle mounted. Each transportable consists of a Kromos Satellite IP Gateway, a VoIP Gateway, an IP video camera, an Anacom Transceiver, and a satellite dish. Some of these stations are equipped with auto acquire antennas that can be pointed to the satellite accurately without manual adjustment for quick deployment.

The basic network is configured to use satellite bandwidth (a precious commodity) only when needed. OES network does not oversee the existing legacy infrastructure. It integrates smoothly both satellite and terrestrial communications to maximize its efficiency. Consequently, a handful of the high priority locations have been assigned dedicated links for continuous dissemination of information.

The entire network is being managed using Kromos NMS, Web, etc. from the Hub location with full authority over the different aspects of such a dynamically formed network. What is more advantageous is that the network administrator also has the ability to manage the network from any other location with connectivity to the network. This raises more the levels of redundancy and survivability of the network.

In conclusion, the Kromos-Anacom network demonstrates the majority of the capabilities that define a Tactical Private Satellite network. It operates with commercial satellites which make it an excellent civilian paradigm. Its proper configuration and successful implementation are said to be proven during a number of recent emergencies involving catastrophic fires, landslides, flooding, and on, where the OES network claims it has been able to respond faster and more reliably with fewer personnel. The State of California Emergency response network, along with many other similar satellite networks, constitutes fine examples of that kind of architecture. They have been used as case studies by more and more organizations which migrates from the public based terrestrial communication infrastructures to their own managed and operated Tactical Private Satellite networks.

b. Military Examples

In addition to the civilian examples of private networks mentioned above, it is worthy to note that there are examples of this type of network within the military domain. Military networks can always be considered tactical due to the fact that the networks directly support military operations. In recent years, the military has sought to utilize satellite communications to enable military units to pass information through the command structure. Even though distances between units are increasing, satellite communications has facilitated this operational flexibility. Each of the networks outlined can stand independently and will, however, most often be employed as a part of a larger network that provides access to DISN services (SIPRNET, NIPRNET, and Defense Switched Network voice traffic) to participating military units. These networks will be examined in the context of their ability to stand alone and to meet the definition of a tactical Private Satellite Network.

The first such network utilizes the currently fielded military owned and operated Milstar EHF satellite constellation and utilizes the AN/TSC-154 Secure Mobile Anti-jam Reliable Tactical Terminal (SMART-T) as the ground terminal. The SMART-T is mounted on a High Mobility Multipurpose Wheeled Vehicle (HMMWV) and will operate in the LDR (756 bps – 2.4 kbps) or MDR (9.6 kbps – 1544 kbps) mode that is supported by the Milstar constellation. The SMART-T will also be compatible with the Advanced EHF constellation. A typical application is to provide range extension of DISN services to units that are beyond the range of line-of-sight transmission systems. Thus, this provides crucial connectivity to widely dispersed forces. The conceptual network diagram in Figure 15 illustrates a SMART-T network as it would be employed by the United States Marine Corps.

By way of description, the outer circles on the diagram represent headquarters or command elements. This diagram does not illustrate the hierarchical foundation of the military organization used to illustrate the SMART-T network in context of a higher level military organization. The rectangle shapes adjacent to the circles represent the SMART-T's that are employed. It is important to note that in the

upper right hand corner, there is a circle labeled “L-Class ship.” This circle represents amphibious ships that have EHF-compatible terminals installed — not the SMART-T.

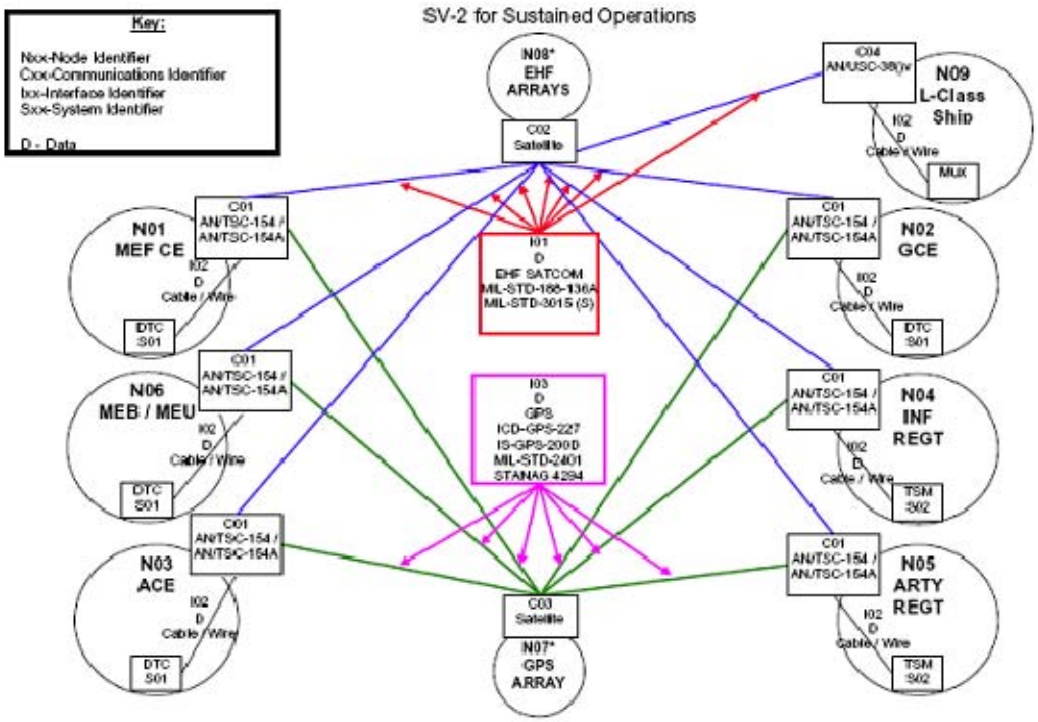

Figure 15. SMART-T Network Diagram (Marine Corps Systems Command).

Tracing the lines that connect the rectangles throughout the diagram illustrates a satellite based private network with all of the participants able to communicate with one another with no connectivity outside of the organization. This network does not have any outside entity exercising control over the network performance and configuration. Therefore, the network participants are able to pass data. This data is limited by the bandwidth provided by the transmission system and the Milstar satellites within their organization or enclave without any outside connectivity. Security for this network is provided by the bulk encryption devices on the SMART-T. Like a commercial private network, the actual space segment is controlled by an outside agency. For a commercial system, the entity controlling the space segment would be the

owner/operator of the space segment, but, in the case of the Milstar constellation, access is ultimately controlled by DISA. The obvious flaw in this particular network is that each SMART-T is single threaded. Thus, if a terminal should fail, the unit relying on the SMART-T for connectivity will have to find other means to access broadband communications networks. Should outside connectivity be desired, users can add an additional satellite transmission system that would provide DISN access and inject that connectivity into the network at any given point. In summary, the SMART-T network is one example of a Tactical Private Satellite Network presently utilized by the military and fits the definition outlined in the beginning of this chapter.

The second military example is the satellite based Support Wide Area Network (SWAN) that has been fielded by the U.S. Marine Corps. The purpose of SWAN is to push broadband communications down to echelons of command that have traditionally not had access to such connectivity. Allowing access to broadband communications allows smaller units to have access to critical information not previously available. An example is live video from Unmanned Aerial Vehicles (UAVs). SWAN utilizes a commercial space segment for transmission and commercially procured ground terminals that have been fielded to military units that, until the recent past, had limited or no access to broadband communications connectivity. The diagram in Figure 16 illustrates the SWAN network for a Marine Division, a subordinate command of the Marine Expeditionary Force:

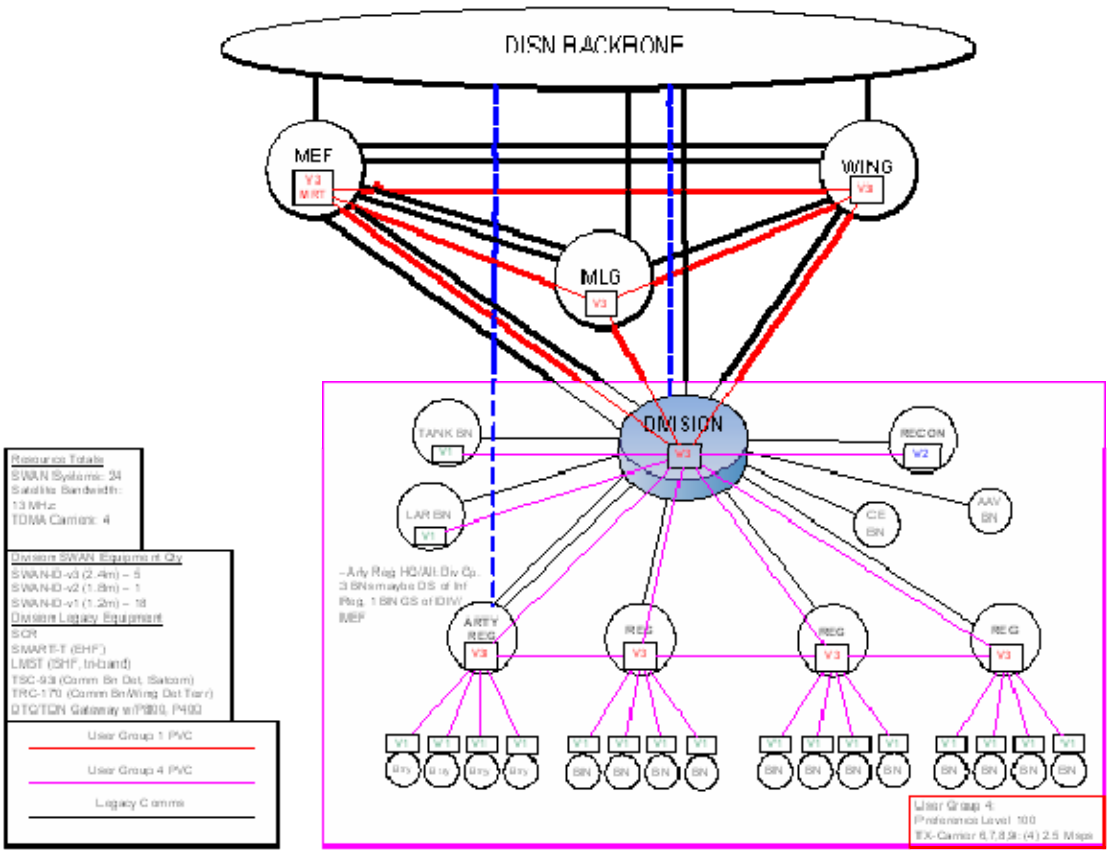

Figure 16. SWAN Network Diagram (Headquarters, U.S. Marine Corps).

Considering only the SWAN terminals in the context of the diagram (the rectangular shapes with a "V" designation in them), the connectivity between the terminals constitutes a tactical Private Satellite Network. Like the examples of civilian networks that were discussed in the previous section, the space segment is owned and operated by a civilian entity with the requisite bandwidth contracted by DISA. As illustrated, DISN services can be injected into the network, as with the SMART-T network, but that is not a requirement for the network to function. SWAN can operate as a stand alone network with each of the users able to communication via a broadband connection laterally as well as up and down the military command structure. The limitations on what kind of information can be passed over this network are constrained by the capacity of the communications link between terminals. There are similarities between SWAN and the SMART-T network in that they are stand alone networks that

provide broadband connectivity to a dispersed user community. The main difference between them is that the space segment for the SMART-T network is managed by the government. Like the SMART-T network, SWAN is a pertinent example of the deployment and use of tactical Private Satellite Networks within the military domain.

2. Capabilities Provided to the User

From the above brief description of both the civilian and military examples, it is easily derived that a Tactical Private Satellite network provides its user with a number of capabilities that go beyond the potentials of the traditional terrestrial, wired, and wireless communication networks or the Very Small Aperture Terminal (VSAT) shared satellite communication solutions. Some of them derived from the "Satellite" aspect of the network which gives true global coverage for the network without the restrictions imposed by the existence — or the lack — of the terrestrial infrastructure; some derived from its "Private" aspect which gives the administrator full authority over the management of the network for the best interest of the owner organization.

The following are some of the most significant features of a Tactical Private Satellite Network that have already been mentioned in the examples above. This accumulative list, which analyzes in further depth the terms flexibility, speed, and redundancy, helps the reader understand why the deployment of such a network is crucial for the organizations who deal with human lives. This also applies to other more profitable ones which cannot afford losses from disrupted communication lines (Business Continuity issues):

- Rapid deployment of the system to sites of incident or opportunity due to the size of the transportable stations and the independence on existing infrastructure.
- Adaptation to the end user environments, no matter how adverse and unfriendly the weather and terrestrial conditions.
- Seamless ubiquitous multimedia services which aims at the true global coverage of the network.

- Network Control Stations with full “authority” over the management of the network. They are proprietary and dedicated to the network without being shared with other organizations which have different targets. These stations manage the network in terms of QoS and allocate the bandwidth on demand for efficient use of available spectrum. Proprietary “hubs” free the whole system from having to rely on shared public networks prone to malfunction and operating failure.
- Restoration of communication (voice, data, and video) anywhere in the network and, many times, from any other location with connectivity to the network. To be more specific, the capability of acting as redundant and sharing load control stations (hubs) by remote terminals empowers them to be used as secondary hubs if the primary one is not available
- Interoperability with the existing terrestrial infra-structure which helps the smooth migration from the emergency to the regular business situation and vice-versa.
- Greater security demonstrated, so far, and higher reliability than radio systems, public networks, and Internet solutions. These networks claim to be less prone to unauthorized access (hacking), virus infections, and disruption in service due to public works.
- Easy installation, operation, and maintenance. As far as the network is “Private,” it is tailor-made to the organization’s specific needs. The ease to operate these networks makes them easy to manage. Since the whole system is simple and uncomplicated to learn, it reduces the time and cost of training the staff on the operation of the network.
- Cost effectiveness and competitiveness with PSTN, radio links, and VSAT shared satellite solutions. This is further justified if the cost, in lives or money, until and for the restoration of communication with the presented solutions is taken under consideration.

Table 4 gives a comparison of the above desirable features with different examples:

DESIRABLE FEATURES	SYSTEM EXAMPLE
Rapid deployment of the system to sites of incident or opportunity	HALO, HughesNet Access Continuity, Kromos-Anacom, SMART-T, SWAN
Adaptation to the end user environments	HALO, HughesNet Access Continuity, Kromos-Anacom, SMART-T, SWAN
Seamless ubiquitous multimedia services	HALO, Kromos-Anacom, SMART-T, SWAN
Network Control Stations with full "authority" over the management of the network	HALO, HughesNet Access Continuity, Kromos-Anacom, SWAN
Restoration of communication (voice, data, and video) anywhere in the network and, many times, from any other location with connectivity to the network	Kromos-Anacom, SWAN
Interoperability with the existing terrestrial infra-structure	HughesNet Access Continuity, Kromos-Anacom, SMART-T, SWAN
Greater security	HughesNet Access Continuity, Kromos-Anacom, SMART-T, SWAN
Easy installation, operation, and maintenance	HALO, HughesNet Access Continuity, Kromos-Anacom, SMART-T, SWAN
Cost effectiveness and competitiveness with PSTN, radio links, and VSAT shared satellite solutions.	HughesNet Access Continuity, Kromos-Anacom, SMART-T, SWAN

Table 4. Comparison of the Different Satellite Networks.

The above list is by no means exhaustive, but it helps highlight the undisputable and invaluable benefits of the proper deployment of a Tactical Private Satellite network in areas where, for some reasons, the so far "conventional" networks' architectures do not suffice — or they lack. What is left for the owner organization is to clearly define its specific needs and the details of the architecture that will best suit its users and potential missions.

B. DESIGN CONSIDERATIONS FOR A TACTICAL PRIVATE SATELLITE NETWORK

There are three primary design considerations that need to be evaluated and considered when formulating the conceptual design of a tactical Private Satellite Network. The considerations that are addressed in this section relate to the inner workings of the network and, in some cases, are completely transparent to the network planner and designer. The considerations that are examined in this section are network availability and data security, a brief comparison between the two most prevalent satellite orbits used for telecommunications and, finally, an examination of protocols and standards associated with the design and implementation of data networks. This section is by no means prescriptive, but it does contain a treatment of relevant issues for the design and implementation of a Tactical Private Satellite Network.

1. Network Availability and Security

There are two major aspects of the Tactical Private Satellite Network that must be addressed by network planners and designers. The first concept is network availability. Availability, with regards to data and information systems, can be generally defined as the accessibility and reliability of data and, in this particular instance, the network and its associated resources and services to authorized individuals in a timely manner (Harris 954). Availability means that the network and the associated services are there when the operator needs it. Obviously, the information that the network is providing and distributing is of a critical nature. Availability is especially critical when considering that timely information flow in a military or ERN operation can have an impact on successful mission accomplishment. There are several means by which to achieve network availability and those are explained as three principles of high availability networking. First, all single points of failure should be eliminated. Single-threaded systems are vulnerable and, by adding redundancy, common cause failures can be reduced. Second, when failures do occur, the network must be provisioned to provide reliable transition from primary systems to back-up systems. Finally, there must be some mechanism

provided to promptly detect failures upon occurrence. This will allow network managers to work more proactively instead of reacting to each issue that occurs on the network (Buddenberg).

The second important aspect with regard to the design and implementation of a Tactical Private Satellite Network is security (confidentiality). Confidentiality, with regards to data and information systems, ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure (Harris 57). Security is absolutely crucial for information in the military domain. Additional security issues become apparent with different types of operations, such as those operations conducted in a coalition environment and operations that are in response to a humanitarian crisis where the military will operate along the side of civil government agencies or non-governmental organizations. Regardless of the situation, security is a crucial element of the network. In this context, the focus is on the security of the data that is being transmitted across the network traversing publicly accessible means. The predominant method for securing data (it will be briefly examined) is end-to-end security. An application of end-to-end security is the establishment of VPNs. Security will be considered within the context of a satellite transmission medium. End-to-end security focuses on the confidentiality, integrity, and availability of data. It is generally media dependent and is achieved by using devices, such as link and packet encryptors augmented by end-to-end security devices that focus on the security of the data itself (Buddenberg). This solution seems optimal when dealing with security because there are adverse issues with regard to link encryption — especially over satellite links that are owned and operated by civilian owned private entities. Link encryption, unlike end-to-end encryption, requires trust relationships between the various users on the network: the end user, the end server, and the satellite gateway. This is not acceptable for data must remain encrypted from the user through the satellite link to the end user. Because there must be a trust relationship to a third party (i.e., the civilian owned and operated satellite gateway), this type of encryption does not seem adequate for transmitting classified or confidential traffic over public resources (Olechma, Feighery, and Hryckiewicz 789). A practical application of end-to-end security is the establishment of a VPN across the

satellite transmission medium. A VPN is essentially a network that appears and functions like a private network to the network end points (i.e., hosts on the network). It uses public resources, such as commercial communications infrastructure to include satellite as the channel between two secure sources (Olechma, Feighery, and Hryckiewicz 785). The value of the VPN over commercial telecommunications infrastructure to the military user is the encryption of all of the traffic from end-to-end. The VPN encrypts all IP data without regard to the application (Olechma, Feighery, and Hryckiewicz 785). Therefore, the VPN provides greater flexibility than other types of encryption that may be applicable to only certain types of applications. The VPN does not discriminate IP data and provides an umbrella of coverage with regard to data. The resulting benefit is that through a VPN, data is encrypted and secure from end-to-end. This is because the resulting VPN architecture places the burden for encryption and decryption on the end user rather than on some sort of gateway that is dedicated to the task of encrypting and decrypting the data (Olechma, Feighery, and Hryckiewicz 785). Due to the utilization of commercial telecommunications infrastructure for this tactical Private Satellite Network, data security is crucial to the successful operation of the network. The establishment of end-to-end security — more specifically the establishment of a VPN — proves to be a viable action to secure sensitive data that would be traversing otherwise unsecured public infrastructure.

2. Examination of Satellite Orbital Characteristics

Having examined the commercial satellite communications capabilities in the previous chapter and, also, having examined the requirements for securing sensitive data over the tactical Private Satellite Network that will traverse commercially owned and operated telecommunications infrastructure, it seems prudent to briefly explain the two prevalent orbital patterns for commercial communications satellites and illuminate the advantages and disadvantages of both types of constellations. The two most common orbital configurations for communications satellites are LEO and GEO. These are certainly not the only two types of orbits for spacecraft, but for the purposes of this research the LEO and GEO orbits are the areas of interest and will be briefly examined.

The following table briefly outlines the advantages and disadvantages of communications satellites that utilize the LEO and GEO orbits:

Orbit	Characteristics	Advantage	Disadvantage
Low Earth Orbit (LEO)	-Low altitude (500 to 200 km) -Orbital period of only a couple of hours -Uses Inter-Satellite Links (ISLs) for continuous communications	-Transponders require less power -Smaller antennas -Fewer transponders required -Delay time is roughly .02 seconds -100% of Earth can be provided with coverage	-Fast moving satellite requires multiple satellites or tracking antennas on ground segment -Numerous satellites required for Earth coverage -Potentially inconsistent or variation in signal delay due to ISL
Geostationary Orbit (GEO)	-Orbit is synchronized with the Earth and rotates in the same direction -Satellite does not move with respect to a point on the Earth's surface -Altitude is about 35,786 km	-Satellite is constant in location -Satellite beams to Earth are motionless -Simplified design for the satellite and the ground segment	-Transponders require high power due to high altitude of satellite -Larger antennas are required at ground segment -Limited to no coverage at high latitudes -Round Trip Time delay of .5 seconds

Table 5. Comparison of LEO and GEO for Communications Satellites (from Gordon and Walker, Principles of Communications Satellites).

Essentially, both types of orbits have advantages and disadvantages relative to their effectiveness of providing communications support to users throughout the globe. In short, the LEO constellations require a large number of satellites for global coverage. For example, Motorola's Iridium constellation has 66 satellites in orbit, but such a constellation can provide true global coverage even in latitudes where GEO satellites cannot "see." Because satellites in LEO are moving rather rapidly, thus equating to a short orbital period (the time required for the satellite to orbit the Earth), LEO

communications satellites must utilize an Inter-Satellite Link (ISL) for continuity of communications. Subsequently, satellites at LEO are more complex because they have to conduct this hand-over the communications signals (Chotikapong, Cruickshank, and Sun 28). Satellites in GEO also have unique advantages and disadvantages with regard to providing communications support. Unlike LEO a satellite, the position of GEO satellites with respect to a particular spot on the Earth does not change. Therefore, fewer satellites are required for Earth coverage, but only at the middle section of the Earth — not at high latitudes. Because GEO satellites do not move and do not require the use of ISLs, their design is much simpler than LEO satellites. In summary, both types of communications satellite constellations, LEO and GEO, provide distinct advantages and disadvantages with regard to providing communications services.

Having differentiated the ways of operating through these two types of orbital configurations, it is worth noting again that one of the strongest new trends in the satellite industry, which also envisions dealing with the problem of overpopulation of specific orbits, is the development of new orbital configurations. This will combine GEO with LEO satellites as a ring constellation to purify the available orbital patterns and take advantage of the strengths of these orbital categories. The commercial space segment that would facilitate the employment of a tactical Private Satellite Network should ultimately be transparent to the organization deploying the network, that is, as long as the bandwidth that is required is available and the VSAT equipment employed is compatible.

3. Networking Protocols and Standards

To complete this section on items and issues for consideration, an examination will be conducted on two prevalent networking protocols and standards and their application for networks — specifically using satellite links for transmission. The two networking standards of interest are Asynchronous Transfer Mode (ATM) and the TCP/IP. Finally, because of its applicability to satellite communications, a hybrid method (combining TCP and ATM protocols) will be examined as well.

The first protocol to be examined is the ATM protocol. ATM is mostly employed on terrestrial networks, but because of the popularity of the protocol, due consideration

must be made within the context of the tactical Private Satellite Network. ATM is intended to transfer many different types of traffic simultaneously. This includes real-time voice, video, and TCP flows of the Internet (Jamalipour 90). Because ATM can handle various types of traffic, it is an attractive method for employment in military-related networks. Here it is common to find various types of data that require transfer from unit to unit over various transmission means. Basically, ATM reduces network overhead by employing fixed size packets. These are called cells. They have a fixed size of 53 bytes and error detection and correction are left to the higher layers of the network protocol stack. ATM has the ability to multiplex and switch data from various sources with varying rates (Jamalipour 90). This multiplexing capability makes ATM attractive for employment in the tactical Private Satellite Network. This is because a single link from unit to unit must be used to pass various types of traffic. Also, a portion of the bandwidth for network management and control functions (this will be examined in greater detail in subsequent chapters) must be reserved. ATM accomplishes the multiplexing by establishing logical connections called Virtual Channel Connection (VCC). All VCCs with a common end point are bundled into a Virtual Path Connection (VPC). This is a series of concatenated Virtual Paths (VPs) and switched along the same route. This creates efficiencies by sharing common paths within the network (Jamalipour 90). Available network bandwidth, however, must be allocated among the VPCs that are running the network. Within an ATM network, bandwidth is logically assigned to a VPC by reserving a portion of the bandwidth on each transmission link for exclusive use of the VPC. This facilitates the rapid establishment of these connections along pre-defined routes (Arvidsson, Berezner, and Krzesinski 1). Finally, a mention of the VP is required to complete the examination of ATM. The important aspects of the VP are that the distinct identity of a traffic strain between tow communicating nodes is recognized and that the endpoint if the VP is not necessarily a computer, but can be another networking device (Arvidsson, Berezner, and Krzesinski 1, Kuehne 7). Because ATM is used on terrestrial networks, it seems logical to take advantage of ATM's characteristics and capabilities over satellite links as well. There are, however, some disadvantages associated with using ATM over satellite links. Generally those disadvantages deal with

the Round Trip Time (RTT) for satellite transmission, the associated latency, and feedback mechanisms for congestion control that will lead to increased probability that ATM cells will be discarded (Hart).

The other networking protocol is the TCP/IP suite. Though there are differences between TCP and IP, they will be addressed as a suite — not individual protocols. TCP/IP is ubiquitous with regard to the Internet. Essentially, data that is processed on a host should end up traversing all of the layers of the TCP/IP protocol stack until it can be transmitted through the physical media and all of the required routing and switching required for Internet access (Jamalipour 92). As noted previously, ATM lets higher layers deal with error detection and correction, but those functions are uniquely a part of the TCP/IP suite. Flow control in TCP/IP is done as an organic function of the protocol stack. TCP/IP performs flow control by dynamic control of windows which allow packets to be transmitted. This is assisted by a feedback mechanism of TCP acknowledgement packets (ACK) packets (Karaliopoulos, Tafazolli, and Evans 334). These ACK packets essentially let the host know that packets sent out were received by the distant end. The value or size of the window mentioned above is a function of the RTT experienced by the particular connection (Karaliopoulos, Tafazolli, and Evans 334). Therefore, an optimal transmitting widow size is directly dependent on the quality and speed of the connection on which the host sits. As with ATM, TCP/IP can be used over satellite links. The performance of TCP/IP, however, is subject to varying conditions relating the physical link itself. As previously mentioned, the two prevalent types of communications satellites are either in LEO or GEO orbits. Also noted previously is the long delay associated with GEO satellites and the potential for variance in the delay of LEO satellites. Weaknesses in the TCP/IP suite are revealed with regard to the use of satellite links. For GEO satellites, the long propagation delay and the variable delay associated with LEO satellites causes the ACK and time-out based congestion control mechanisms of TCP/IP to perform weakly (Jamalipour 101). The bottom line with TCP/IP over satellite is that there are numerous problems associated with the physical link — in this case, the satellite link — that adversely affect the congestion control mechanisms associated with TCP/IP. To mitigate the affects of long propagation delay transmission medium on TCP/IP,

considerable research effort has been devoted to enhancing the performance of TCP/IP in this environment (Karaliopoulos, Tafazolli, and Evans 334). The Internet Engineering Task Force (IETF) has issued Requests for Comment (RFC) relating to congestion control and performance of TCP/IP over satellite. The following table briefly outlines the efforts of the IETF with regard to this issue.

Date Issued	**RFC**	**Title**	**Description**
May 1992	1323	TCP Extensions for High Performance	Presents a set of TCP extensions to improve performance over large bandwidth delay product paths and reliable operation over high-speed paths
January 1999	2488	Enhancing TCP Over Satellite Channels using Standard Mechanisms	Inclusion of IETF standardized mechanisms that enable TCP to more effectively utilize available network capacity
April 1999	2581	TCP Congestion Control	Defines TCP's four intertwined congestion control algorithms
February 2000	2760	Ongoing TCP Research Related to Satellites	Outline of possible TCP enhancements that may allow TCP to better utilize the available bandwidth provided by networks containing satellite links
September 2000	2914	Congestion Control Principles	Explains the need for congestion control on the Internet
December 2002	3449	TCP Performance Implications of Network Path Asymmetry	Description of TCP problems that arise because of asymmetric effects of bandwidth asymmetric networks and packet radio sub-networks
June 2005	4057	IPV6 Enterprise Network Scenarios	This document describes the scenarios for IPv6 deployment within enterprise networks. It defines a small set of basic enterprise scenarios and includes pertinent questions to allow enterprise administrators to further refine their deployment scenarios.

Table 6. List of Applicable Request for Comments (from http://www.ietf.org/rfc.html).

After briefly examining the apparent strengths and weaknesses regarding ATM and TCP/IP, and their use over satellite networks, it would be useful to consider the hybrid protocol of using TCP/IP over ATM and satellite links. The best of both protocols can be used to create an efficient and effective means for the transmission of various types of traffic (real-time voice and video included) over a satellite link where propagation delay is either excessive or unpredictable. The goal of the Tactical Private Satellite Network is to get broadband network capability to deployed users where there is no mature wired infrastructure by utilizing commercial satellite communications. To achieve the goal of broadband satellite networks, the integration of TCP/IP and ATM needs to be seriously considered (Jamalipour 95). The issue is how to integrate TCP/IP datagrams into the ATM cell structure. For the proper integration of the protocols, TCP/IP traffic must be transmitted with the fixed size of the ATM cell and transmitted through the Virtual Channel (VC) that is set up by the ATM network for data transmission. An inherent problem is that there can be a limited number of VCs and that number is ultimately controlled by Quality of Service (QoS) manager on the ATM network (Jamalipour 95). For TCP/IP traffic to be packed into ATM cells, a mechanism within ATM must somehow pack the TCP/IP datagrams at the sender and unpack them at the receiving host to fit TCP/IP. That is done by the ATM Application Layer (AAL) and, with the case of TCP/IP traffic, AAL 5 (Kuehne 12). There are total of five AALs — each with a different function. Specifically, AAL 5 is the primary AAL that supports connection-oriented and connectionless data (Cisco 27-10). TCP is connection-oriented and IP is connectionless. Therefore, this AAL is applicable to the packing of TCP/IP into ATM cells. The confluence of TCP/IP and ATM provides a mechanism for taking advantage of the best of each protocol for transmitting data over less than ideal satellite links.

After an examination of desired attributes of the network; availability, and security, as well as an examination of the advantages and disadvantages afforded by the two predominant orbital configurations for communications satellites — LEO and GEO —, and a treatment of the prevalent networking protocols, the portion of this chapter will be devoted to defining the desired physical attributes for a Tactical Network Entry Point.

This is the deployable base station that acts as the hub for the Tactical Private Satellite Network. There will be a comparison to similar systems and the operational implementation of the tactical Private Satellite Network in the context of common military missions.

C. TACTICAL NETWORK ENTRY POINT

1. General Capabilities of the Conceptual Network Entry Point

a. Physical vs. Logical Entry Points – Design

The key operational consideration for the Tactical Network Entry Point that will be examined in this section is the concept that this base station will have two distinctly different network entry points: a physical and a logical entry point. The logical entry point, however, is broken down into two separate and distinct entry points for the purposes of data transfer and network management. The differentiation between these two types of entry points is significant to this work in that the physical apparatus represents the hub of the Tactical Private Satellite Network. The data traversing the network is further segregated to separate network management and control functions from the majority of the other data that the network is transferring between network members.

The first type of entry point that will be examined is the physical entry point. The physical entry point functions as the hub of the network and as the Network Control Station (NECOS) for the Tactical Private Satellite Network. With regard to the physical entry point of the NECOS, the base station controls the physical connection between the base station and subordinate terminals and lateral communications between each of the subordinate terminals. Noting that this network utilizes satellites to achieve the desired connectivity, it is implied that the base station will be able to control the ability of the subordinate terminals to access the space segment and join the network by utilizing permissions similar to those required by DISA to join and operate on the MILSATCOM network. Therefore, some level of authentication would be required by both the base station and subordinate terminals. The physical topology of the network that resides behind the base station and subordinate terminals is somewhat generic from

the perspective that no special networking devices, not readily available in the commercial marketplace, are required for the network to be extended to users from the satellite terminal. The only exception to this would be any mandated encryption devices, such as those required by DISA. Figure 17 illustrates a sample physical topology for the Tactical Private Satellite Network:

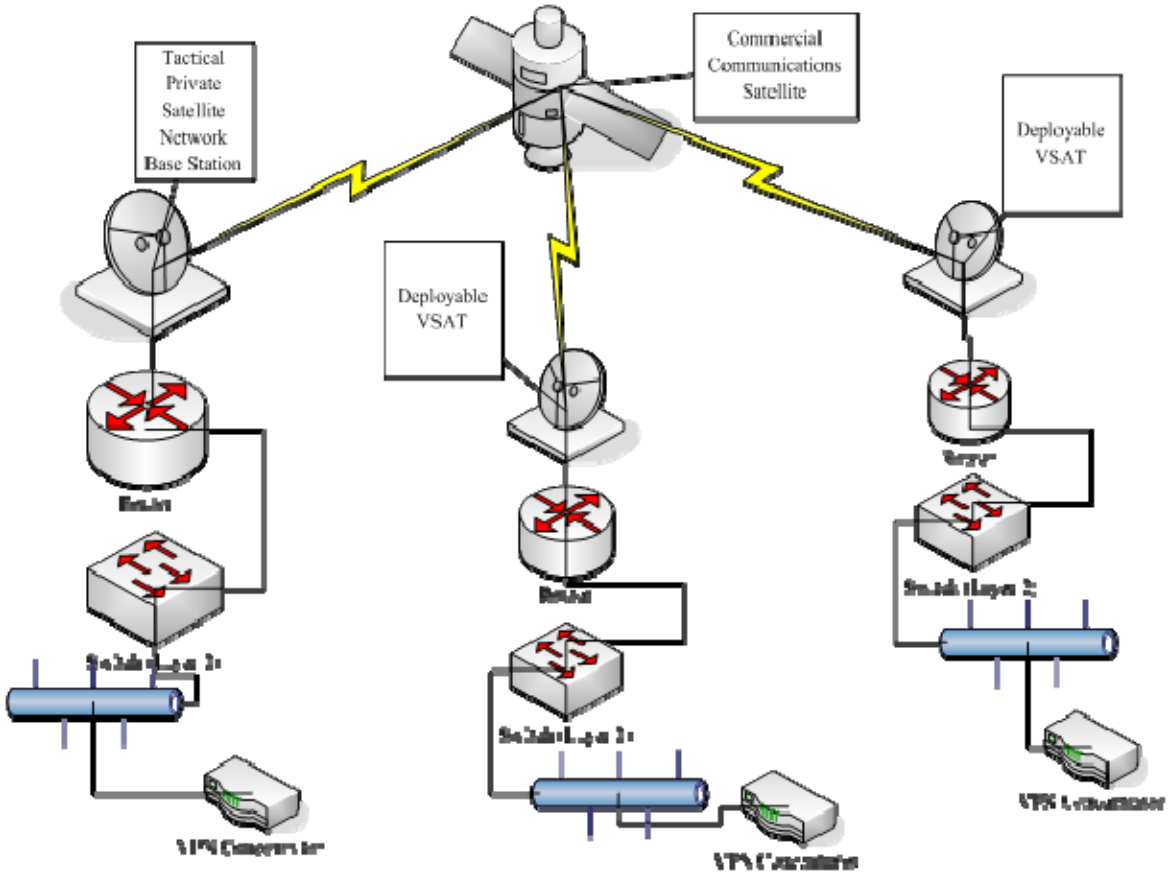

Figure 17. Sample Physical Topology for the Tactical Private Satellite Network.

In this illustration, basic networking components (switches, routers, wireless access points, Virtual Private Network concentrators, and user hosts) could all be connected to the satellite terminal (including the base station) in any combination to extend the network to the required user community. The actual physical architecture would ultimately be decided by the unit operating the network based on the mission, the

information exchange requirements, and the equipment available for use. The key is that the user maintains some flexibility with regard to the physical topology of the network based on determined information exchange requirements and the aggregate bandwidth provided by the satellite link.

In addition to providing the physical access or entry into the Tactical Private Satellite Network, the base station also maintains functionality above that of the subordinate terminals. The other functionality is in the form of the logical entry points for the network. The logical entry points function in a similar fashion to the physical entry point in that the NECOS can exercise control over the performance and operation of the network.

To that direction, there are two logical entry points. The first logical entry point is to control the physical connection between the base station and subordinate terminals and the satellite as well as provide a network management control channel through which the network devices can be remotely managed. This logical entry point addresses the desired functionality in this model of the NECOS to allocate satellite bandwidth between terminals. There are instances where some terminals will be required to send and/or receive large amounts of data relative to the other terminals on the network. Ideally, the NECOS should be able, when the situation arises, to either allocate bandwidth between both the base station and a subordinate terminal, or between subordinate terminals manual, or set some parameters for the dynamic allocation of satellite bandwidth. In addition to managing the satellite bandwidth within the network, the network management control channel would be utilized to remotely manage network devices that were deployed and connected physically to subordinate satellite terminals. Conceptually, the NECOS could dictate QoS requirements for the network and utilize SNMP to maintain the overall health of the network. The concept of remote network management will be examined in greater detail in Chapter V. The second logical entry point is for all of the other data to travel to and from the terminals and network devices that are deployed. Simply, it is the logical path for connecting clients to servers of the application and data services that are operating on this particular network.

Because there is a need for two separate logical entry points (network control and general data), each can be considered a separate channel and, therefore, some method must be used to separate the two. Again, this study is not prescriptive but merely providing information on how the logical entry points may be kept separate. There are two ways in which the logical entry points can be established within the single transmission aggregate. One way is to introduce a multiplexing device between the satellite terminal and network router. The other way is by taking advantage of the Virtual Circuits that are operating characteristic of ATM. Either way, the data channel and the network management control channel can be established and kept separate from each other. Figure 18 depicts the logical entry points for the Tactical Private Satellite Network. This multiplatform control, separation of control and data links, for generally reconfiguring the nodes or the whole networking segment of self-forming networks, has a fundamental role in cases of tactical networks (Bordetsky and Bourakov).

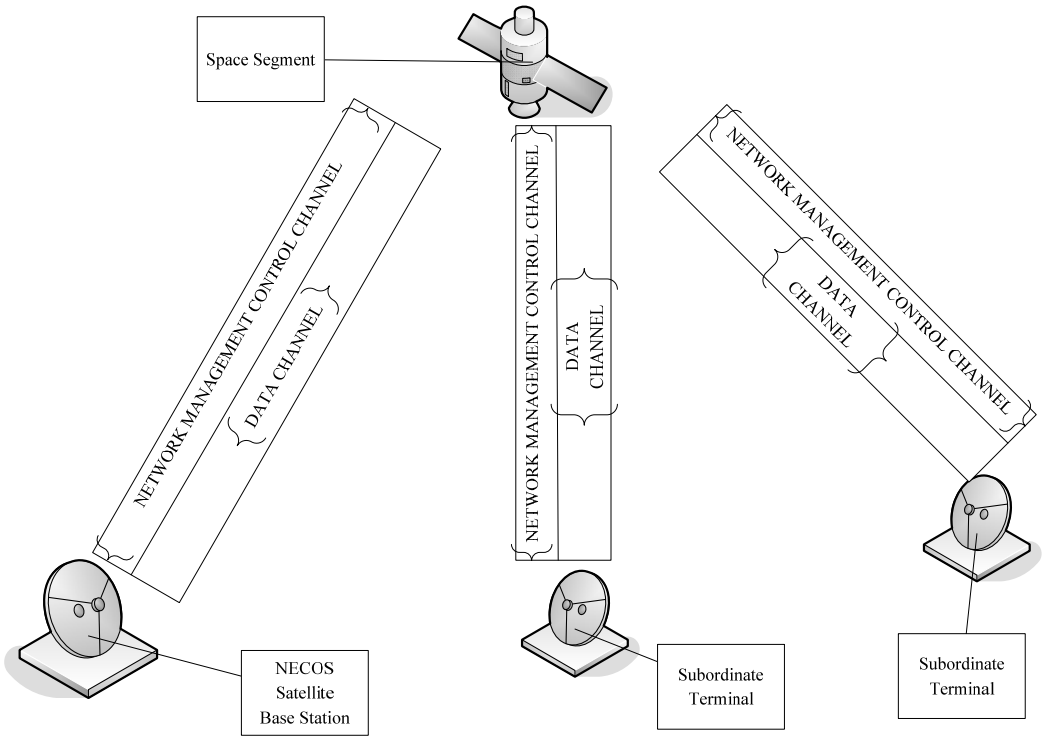

Figure 18. Depiction of the Two Logical Entry Points.

Ideally, as the illustration depicts, the aggregate satellite bandwidth would be apportioned between the two logical entry points. Considering that the data channel must contain the majority of the bandwidth — most of the traffic traversing the network will do so via this data channel —, the network management control channel can be smaller relative to the data channel. As mentioned above, a more in-depth treatment of the data channel will be done in Chapter V.

In summary, the Tactical Network Entry Point provides functionality not present in other satellite terminals on the network. The physical entry point is the gateway to the network and provides physical access to the space segment. In addition to the physical entry point, the base station also provides, through the implementation of specific network protocols or hardware, two logical entry points. One logical entry point is considered a network management control channel that is used to control satellite bandwidth and manage deployed network devices remotely. The second logical entry point is a channel specifically reserved for the transfer of data from one part of the network to another. This separation of the aggregate satellite bandwidth is crucial to the user by providing a greater amount of operational flexibility in terms of network deployment, operation, and management.

Further research needs to be done on the data forms of the different categories. Data to be transferred will need, in many cases, to be encrypted. This may be an additional and almost useless overhead for the management data. On the other hand, all data, including management data, needs some kind of “need to see” configuration. This will be implemented by the identity management device which will govern the network in terms of who is eligible to participate and who is not. In any case, additional devices need to be added to the above simple infrastructure to complete the communication scheme of the Tactical Private Satellite Network.

b. Requirements and Characteristics for a Conceptual Tactical Network Entry Point

After the above descriptions of Network Entry Points and the separation between physical and logical ones, it is well understood that this research shows that the

Tactical Network Entry Point is the base station of the Tactical Private Satellite Network that serves the function of NECOS for the network. The conceptual capabilities of such a "hub" should be in accordance with the functions and performance that users should expect. Conceptually and very concisely, NECOS will control the network by providing monitoring and control of the widely dispersed earth stations. At this point, it needs to be repeated that the satellite bandwidth is allocated by the service provider. Nevertheless, the gateway device will be capable to apportion the allocated bandwidth within the network to facilitate information exchange. Basically, the concept is that once the bandwidth is acquired, there is no requirement for civilian owned/operated IP services. This, in concert with the employment of the gateway device which allows for the control of the bandwidth, is a fundamental benefit of the Tactical Private Satellite Network.

To be more detailed, at first — and from the nature of the operations for which this research designed the network –, it is expected that the base station will be easily deployable for vehicular, shipboard, and man-portable configurations. This is because the Tactical Private Satellite Network can be implemented in a variety of operational scenarios. Flexibility of where and how the base station can be operated is essential. Depending on the operational application, this also includes an On-the-Move (OTM) capability (potentially).

The functions that the base station is expected to perform are elaborate. This is because it would deal with the management of a significant and crucial, in terms of human lives, network. For that reason, it will require knowledgeable operators to conduct those operations. Yet, and for the sake of operational flexibility and ease of deployment, it should not require enhanced skills to install and conduct basic functions of the system.

The base station should be able to have large enough bandwidth to serve as a broadband communications pipe between subordinate stations. This will ensure that the network can be used for C2 purposes and allow for the establishment of a control channel that would be used for remote management of network devices. As it has been discussed in the above paragraphs, through its performance as network management and a gateway access, it will give the communication architecture the ability to act as a

broadband, on-demand global Internet based on IP. This will incorporate key emerging network technologies, such as QoS provisioning and bandwidth guarantees. Thus, it will allow warfighters access to the GIG anywhere at anytime.

From the scope of technology, the base station should be generic in nature (technology agnostic) so that different types of VSAT users can connect to the network. In other words, the base station should be compatible by frequency band and Media Access Control scheme instead of some proprietary means that would only limit its interoperability with others.

The overall functionality of the base station provides the capability to use multiple different satellite frequency bands, ideally simultaneously, to enhance operational flexibility. For that reason, it should be designed with dual antenna systems so it can support two simultaneous separate satellites to terminate deployed terminals and be capable of operation on multiple bands simultaneously. This can serve also another cause: the base station can on the same time relay everything to existing permanent stations which are positioned in different satellite footprint than the VSATs.

Moving to the “pure” management side of its functionality, the base station should be ideally able to control the modems on the subordinate VSAT terminals. This is to dynamically allocate bandwidth between the terminals within the network and to set QoS parameters to get efficient use out of the bandwidth allocated for the entire network. Generally speaking, bandwidth, throughput, timeliness (including jitter), reliability, perceived quality, and cost are considered as QoS metrics in telecommunication networks (qtd. in Jamalipour 99). In addition, latency, interactivity, prioritization, and high availability are considered QoS attributes. Of course, this does not literally mean to control the transponders on the satellite; rather, this means to adjust the parameters of the modem. For example, bandwidth allocation and congestion control are few of the critical factors in effectively providing management service. Furthermore, the management allocated bandwidth must also incorporate a way of communication (voice or text in the form of collaborative communication, such as “chatting”) between the users and the administrator into the base station. This is so the latter can inform the local users of the problems so they can fix them or so they can conduct helpdesk services.

Following the trend of the modern communication protocols, it shall be designed with a pure Everything over IP (EOIP) architecture such that deployed tactical users achieve “IP mobility” without system reconfiguration — no matter when and where they enter the area of interest.

In terms of the overall topology in which the base control station contributes by managing the network, clarification of the basic principles of hierarchy of this whole system and the addition of a multipurpose asset as the base station must be stated. Generally, a group of satellite terminals may be regarded as constituting a Network and arrangement of their communication links as the Network Architecture or configuration (Celic, 177). The architecture, however, of a satellite communication network is different from most terrestrial networks: all links pass through a satellite transponder that will see all earth terminals within its coverage area. A single satellite network may, therefore, be regarded as a star topology with the satellite transponder as the central node. The transponder, however, is generally transparent and it is the logical connectivity and topology of the users which is of interest. This will generally be either a Star configuration — with a large hub station — or a Mesh configuration where there is effective equality between all terminals. Figure 19 shows the architecture distinction:

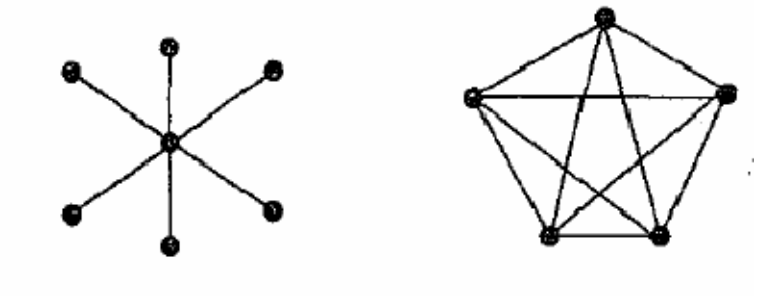

Figure 19. Hub and Mesh Architectures.

As well as the user links, there will be distinct Network Management functions handled from NECOS (base station). This is usually based upon a start configuration. Because NECOS functions as Gateway (hub in sociological terms) between satellite ground terminals and other satellite ground terminals and terrestrial

telecom networks, there can be no equality between it and the other VSATs. Consequently, for the earth components of the Tactical Private Satellite network, there is a Mesh configuration among the VSATs for point to point communication and a Star configuration for the communication with the base station which acts as their gateway to DISN GIG (NIPRENET, SIPRENET, and World Wide Web). It also manages each of them so it can guarantee the quality of communication.

Another characteristics/capability for the network entry point warrants examination. The ability for the base station to control access to the satellite medium is critical to the implementation of the Tactical Private Satellite Network. Conceptually, the base station will provide access to the space segment and the associated bandwidth. It will, thus, perform a gateway function. There are several models for Media Access Control (MAC) that could be applied to the gateway system, but the model that is deemed as the most appropriate for implementation is a MAC similar to the one utilized by the 802.16 standard.

There are several reasons why the implementation of 802.16 MAC is an attractive candidate for incorporation into a conceptual gateway device. The first reason is that the 802.16 MAC is designed to support broadband wireless point-to-multipoint access (multicast) applications and a variety of services, such as bursty and continuous traffic (Eklund, et al., 99). The multicast access described is the same access that will be required of the Tactical Private Satellite Network. This is where multiple stations will be connected to the base station/gateway and to each other via the satellite (wireless) link and will be required to pass various types of traffic through the routable network. Second, 802.16 MAC supports a variety of backhaul mechanisms. This includes ATM and IP traffic (Eklund, et al., 99). Depending on the operational implementation of the Tactical Private Satellite Network, there may be different options for backhaul as well. This is why this particular issue is of interest. The third issue deals with transport efficiency. Transport efficiency is critical — especially in satellite communications networks — because here there is a finite amount of bandwidth available to users within the network. An efficient method is, therefore, required to allocate bandwidth within the network user terminals. Because the modulation and coding schemes are specified for a burst profile

(this may be adjusted adaptively), the 802.16 MAC can make use of more efficient burst profiles during favorable link conditions. It may also reduce efficiency to increase reliability when less than favorable link conditions occur (Eklund, et al., 99). Here is another example where the properties of the 802.16 MAC are attractive for implementation in the conceptual network framework. The ability to manage the actual communications link (in the case of this work, the satellite link) is critical to the implementation of the Tactical Private Satellite Network. Therefore, the final issue that will be examined is the management capability provided by the 802.16 MAC. To discuss the management capability provided by the 802.16 MAC, it is necessary to briefly look at the 802.16 MAC Protocol Data Unit (PDU). The PDU for the 802.16 MAC consists of a MAC header of fixed length (a generic header and a bandwidth request header), variable payload, and a cyclic redundancy check (CRC). Management PDUs do not contain any payload; rather, they do contain MAC management messages (Eklund, et al., 102). Because there are management-related messages incorporated in the MAC PDU, this would eliminate any additional overhead caused by having to use some other method to conduct Media Access Control as well as centralize the management of a point-to-multipoint link. This is similar to the topology suggested for the Tactical Private Satellite Network.

In summary, the base station device that functions as the gateway for the Tactical Private Satellite Network must be able to perform, in addition to the other tasks, Media Access Control to control access to the commercial satellite link. This functionality is critical because the finite resource of the satellite bandwidth must be apportioned to all stations on the network. It must provide security at the physical layer. Because 802.16 MAC can take advantage of fragmentation and bandwidth allocation processes, it can serve to maximize the overall link efficiency, effectiveness, and flexibility (Eklund, et al., 103). Due to the characteristics of the 802.16 MAC, a similar control mechanism would be a desirable quality to incorporate into the Tactical Private Satellite Network.

In terms of power and judging by mission, it will not only have to utilize a self-sustained power generator, due to existing conditions in the deployment area, such as

lack of or damaged terrestrial infrastructure, but also the capability to migrate to commercial power source when the power lines in the area can be found or restored.

It is also prudent to recognize that such an empowered base station (Network, Management, and Control) forms a Single point of failure. Therefore, use of a Standby Hub Earth Station is necessary. It must be developed to have reduced capacity to take over in the event of a main control station failure. The main and stand by control stations will be connected to each other to maintain replication of pertinent database information at each site.

As clearly perceived by the above requirements, NECOS will be responsible for the management of the total Tactical Private Satellite Network as a system. It will manage and control the system resources and provides overall system administrative functions. Overall and beyond the role of transmission and relay of communication (data channel function), as a communication gateway it will provide services, such as addressing and routing, information assurance, end-to-end QoS, and general network services to and across the Tactical Private Satellite Network as a type of Edge network.

There is great value associated with the operation of such a multitasking and complete ground control station. Consequentially, a great number of attempts have been made to that direction by different military branches to guarantee the communication lines through satellite connections during their dispersed type of missions. The next few paragraphs will be a brief review of how two of the most relevant (to the type of missions examined here) commands intend to deal with the use of Tactical Satellite Networks in terms of establishing and managing them with the use of the proper gateways, or NECOS, for the purpose of this research.

2. Comparison with Other Gateway Type Systems

To build the C2 node on the battlefield, four things are needed: a network path, network services and capabilities, applications that write and provide those functions, and a number of sensors. Those four pieces must be sized or provisioned to any platform — whether a command post, an HMMWV, or a ship. This summarizes more or less the concept of a Communication Gateway (CGW) which is not new, but also not something

trivial to build and implement. Different military branches have evolved different CGW approaches to provide flexible communications networks for transition between stationary and maneuver operations. The use, however, of a CGW that includes satellite assets gives to the flexibility dimension a different and more powerful meaning. It supplies the mobile capability and, at the same time, provides an over-the-horizon capability to bring in a common operational picture to all units on the battlefield — no matter distance or different obstacles which interrupt or even forbid communication through the direct conventional communication lines. It provides the very last deployed unit with real-time information and, at the same time, enriches the holistic tactical picture of the stationary command posts which may be positioned hundreds of miles away from the area of current operations. The ultimate goal is the building of a Common Operational Picture (COP) and Situational Awareness (SA) access among geographically separated maneuvering forces and stationary C2 nodes. The goal is to empower the edges, but without depriving the command posts of real-time tactical picture of the deployed units.

To that direction, the next paragraphs give a brief description of a few CGW systems with satellite connectivity that not only give to the warfighter real-time tactical information, but also provide access to DISN services (SIPRNET, NIPRNET, and Defense Switched Network voice traffic). The different aspects of each of them will be emphasized to form a clear picture of the individual advantages and disadvantages of those systems that facilitate and enhance dispersed tactical operations.

a. Command and Control On-the-Move Network Digital Over-the-Horizon Relay (CONDOR) – United States Marine Corps (USMC)

CONDOR system is a bridge strategy that USMC has developed to get around C2 problems. To be more specific, the recent operations showed that there is a major problem with the dissemination of information around the battlefield using the tactical data radios, Enhanced Position Location Reporting System (EPLRS), which limits the communication to line-of-sight distances. That proved to be a significant issue in operations, such as Iraqi Freedom where the units expanded 60 or 70 kilometers a day and, thus, broke that line of sight. Also, into a mountainous region, such as Korea, that

line of sight is constantly, due to terrain masses, being broken. As Col. Wilson stated, from the above needs, CONDOR emerged to bridge these EPLRS communities over a distance and fix the specific problem in the Marine Corps (qtd. in Lawlor). Simply put, CONDOR uses commercial off-the-shelf equipment to link existing Marine Corps radio systems and data networks and provides the over-the-horizon communications capability necessary to link EPLRS users. A great portion of the CONDOR system involves deploying mobile platforms that can use satellite links when terrestrial radio networks are out of range. This maintains situational awareness and connectivity to tactical data networks and applications.

CONDOR was initially developed as a digital communications relay for On-the-Move/Over-the-Horizon (OTM/OTH) data communication, but it is more than that: it creates an in-theater commercial satellite intra-network to connect Below Regiment "On the pause" C2 Nodes and provides sustained SIPRNET connectivity throughout displacement (Wilson). More specifically, the requirements for building such a CGW system were:

- Digital data transfer – Stationary to Maneuver C2: While Stationary Command Post locations (Brigade and Above) enjoy broadband digital transfer (up to Megabits per second (Mbps)), the maneuvering units (Brigade and Below) are reduced to less than 10% of this with tactical radios or L-band transceivers.

- No New Radio Capabilities until JTRS: Joint Tactical Radio System (JTRS) will add the Wideband Networking Waveform (WNW) line of sight (LOS) radio capability but the estimated fielding of sufficient JTRS quantities is no earlier than 2015-2020.

- OTM/OTH Issue: Users demand reliable COP and SA access between geographically separated Maneuvering forces that are similar in scope to Stationary C2 Nodes.

- Platform Integration: C2 Nodes require integration for network services on multiple platforms.

- Military Satellite Bandwidth Saturated: The system can work with dedicated military satellites, but it needs to be able to route communications from existing EPLRS line-of-sight radio networks to available bandwidth from commercial satellites.

The above requirements composed the ultimate goal of CONDOR which is to enhance SA for maneuvering elements while they are OTM and to provide a communications path to higher headquarters that is not constrained by LOS limitations and operates OTM. CONDOR capability sets include a Gateway which is a tactical vehicle providing OTH and on-the-move OTM digital communications to a maneuvering EPLRS data community; a CONDOR Point of Presence Vehicle (PoP-V) which is a tactical "Point of Presence" Vehicle providing OTH and OTM digital communications with Turbo Diesel Registers (TDR) and a CONDOR Jump C2 Variant (JC2-V). More specifically, the components of CONDOR system are:

- CONDOR Gateway which connects Mobile C2 Networks OTH/OTM: It fits into a single transport box and allows Marines to take the information on an EPLRS radio off of the network in one location, move it through a router as an IP datagram, and pour it over a satellite link into another geographically separated EPLRS network. The prototype comprises an EPLRS radio, a router, and a command and control personal computer (C2PC) gateway tied into an Inmarsat radio that has an on-the-move antenna on top of the vehicle. At this point, this thesis needs to emphasize that CONDOR is technology agnostic and can rely on Inmarsat, Ku-band, Ka-band, Iridium, or any other technology for connectivity.

- CONDOR Point of Presence (PoP-V) which enables the use of all Tactical Radios to enter C2 Mobile Networks for CONDOR access: The above gateway technique works for units that carry EPLRS radios, but not for the ones that do not have this equipment. In general, because these units are outfitted with legacy equipment, such as the Single Channel Ground and Airborne Radio System (SINCGARS), HaveQuicks, high frequency automatic link establishment or tactical satellite Demand Access Multiple Access (DAMA) systems, a CONDOR point of presence was created to solve this problem. Its main function can be described as, in one hop, information from the sensor

or the shooter is taken to the CONDOR point of presence and from there to the regiment. The latter breaks it up and puts it into the major subordinate command so units have lots of bandwidth to move. With that, units are offloading the bandwidth-limited maneuver element command and putting all the information into the major subordinate command until it needs to come down and move to its recipient. More or less, "it's a bandwidth multiplier on the battlefield," as Colonel Wilson explains and, because the four legacy radios use the same waveforms that will be placed in the JTRS, the CONDOR point of presence is nothing more than the JTRS when it is available.

- CONDOR Jump C2 Vehicle, which provides sustained SIPRNET connectivity throughout displacement: The final portion of the CONDOR effort envisions solving the communication problem that commanders face when they change locations. Nowadays, a commander must rely on single-channel radios or small satellite systems to maintain the common operational picture and command and control while in transit. To solve this problem, the CONDOR team developed the Jump C^2 Vehicle concept. Secret Internet protocol router network and non-secure Internet protocol router network servers would be incorporated into the vehicle. When a commander must change locations, communications personnel would turn on these servers and synchronize them with the servers in the current command post. As a result, commanders would be able to continue to see databases and receive current information.

As already mentioned, one of the biggest advantages of CONDOR is that it is technology agnostic and does not rely on a particular satellite technology for OTH communications. Any technology for connectivity is good either comes from military dedicated Ku- and Ka-band satellites or from commercial assets (Iridium, Inmarsat, and on). Thus, it deals even more effectively when military satellite bandwidth is not enough to cover every single military need. For the sake of military commanders, it also brings the benefits of using already existing commercial bandwidth.

There are other benefits related to CONDOR. With the evolution of JTRS and CONDOR, JTRS would blend technologies in a hierarchical access fashion for both scalability and redundancy. This is similar to the design of a mesh network with multiple

communication hubs at multiple levels able to communicate with each other and to end nodes. If one or more hubs are lost, redundant paths are available to continue to carry traffic. CONDOR is designed to eliminate the single-point-of-failure problem by providing three different communications paths. This includes satellite bandwidth, UAVs, and ground relays (Mohney).

It also demonstrates the potential option of using UAVs, such as the Predator, flying as an overhead relay. This is because, from an integration standpoint, CONDOR can be plugged into any vehicle the Marines operate — ranging from the simple Jeep to its next-generation high-speed amphibious fighting vehicle.

In terms of network management, CONDOR uses the allocated commercial bandwidth, but without having the ability to interfere with management functions. The only efforts that have been made so far are to improve the quality of transmissions by removing the effects of disruption generated by the constant maneuvering of the units. To that direction, Disruption Tolerant Networking (DTN) is evolving to help maintain reliable communication across periods of unreliable connectivity through in-network store-and-forward. Its main strategy will be to incrementally move messages closer to the destination, with a technique called custody transfer, in a store-and-forward manner using local storage at intermediate nodes — instead of relying upon an end-to-end stable path — to ultimately deliver messages with reduced latency and higher throughput (Parikh and Durst, 1). Its main advantage is fully exploited for data transfers where the time-value of the information exceeds the durations of disruption. For the purpose of network management, DTN will be an automatic feature in the form of a gateway into the CONDOR units without leaving flexibility for other management functions. Figure 20 gives a brief picture of the CONDOR's architecture and its main weaknesses.

To summarize, CONDOR system demonstrates CGW capabilities that are desirable not only for the dispersed MSSC units operating under adverse conditions far away from their headquarters, but also for any kind of Tactical — military or not — situation where the need for high quality and constant communication lines cannot rely on existing terrestrial infrastructure. What makes it highly relevant to the subject of this

research is that it can use commercial satellite technologies without jeopardizing the security of the mission. From the network management perspective, the downside of CONDOR, as it appears so far, is that it does not give any management capabilities to its users when using commercial bandwidth and only works with the allocated portion.

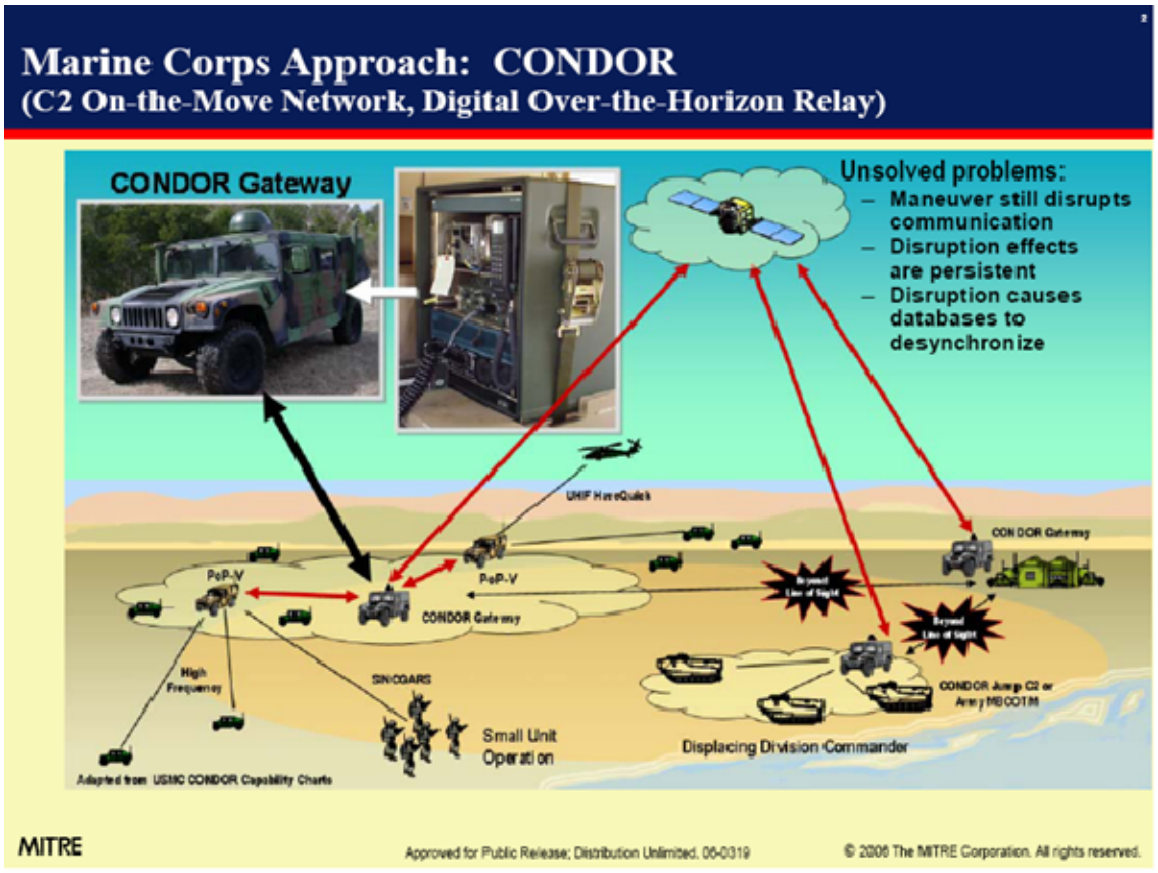

Figure 20. CONDOR Architecture (from Durst et al., 2).

b. Mobile SOCOM Strategic Entry Point (M-SSEP) – United States Special Operations Command (USSOCOM)

USSOCOM is one of the agencies that have understood the significance of having true global and uninterrupted communication coverage to expand the area of operations beyond the reach of one of the current six regional SSEP around the globe. For that reason, a new project has been initiated to evolve the M-SSEP (USSOCOM).

From a very first approach of the requirements specification document, the general description of the M-SSEP is a communications terminal that will support Special Operations Forces (SOF) that are unable to draw services (voice, video, and data) from one of six Regional SSEPs, or support surge operations, when an existing Gateway/Teleport or SSEP cannot support SOF assets deployed in theater. It will provide seamless access to government and commercial satellites operation in X, C, Ka, and Ku bands simultaneously. It envisions to provide SOF Commanders the ability to consolidate C4I transmission systems and services (Black/Red/Grey Voice, VTC, and Data) required by SOF through a theater SSEP during surge operations or when an existing gateway cannot support termination.

More specifically, the M-SSEP can be deployed anywhere in the satellite footprint of the region requiring support. It shall support operations in a stand-alone configuration or co-located with a SSEP to provide SOF Information Enterprise (SIE) services to tactically deployed SOF. It will be developed with an EoIP (voice, video, and data). The M-SSEP will provide multiple interfaces for connectivity via commercial Circuits or DISN GIG.

The following figure gives a rough picture of the architecture of a gateway such as M-SSEP. As it can be seen by the figure, M-SSEP shall be capable of terminating multiple satellites — a minimum of two per M-SSEP and a minimum of six networks per type of terminal. With that configuration, it will be able either to support surge operations and keep services locally in theater or to augment existing SSEP operations, but without providing services to local users. In either case, it shall interface with DISN GIG or standard commercial telecommunications circuits for terrestrial transport.

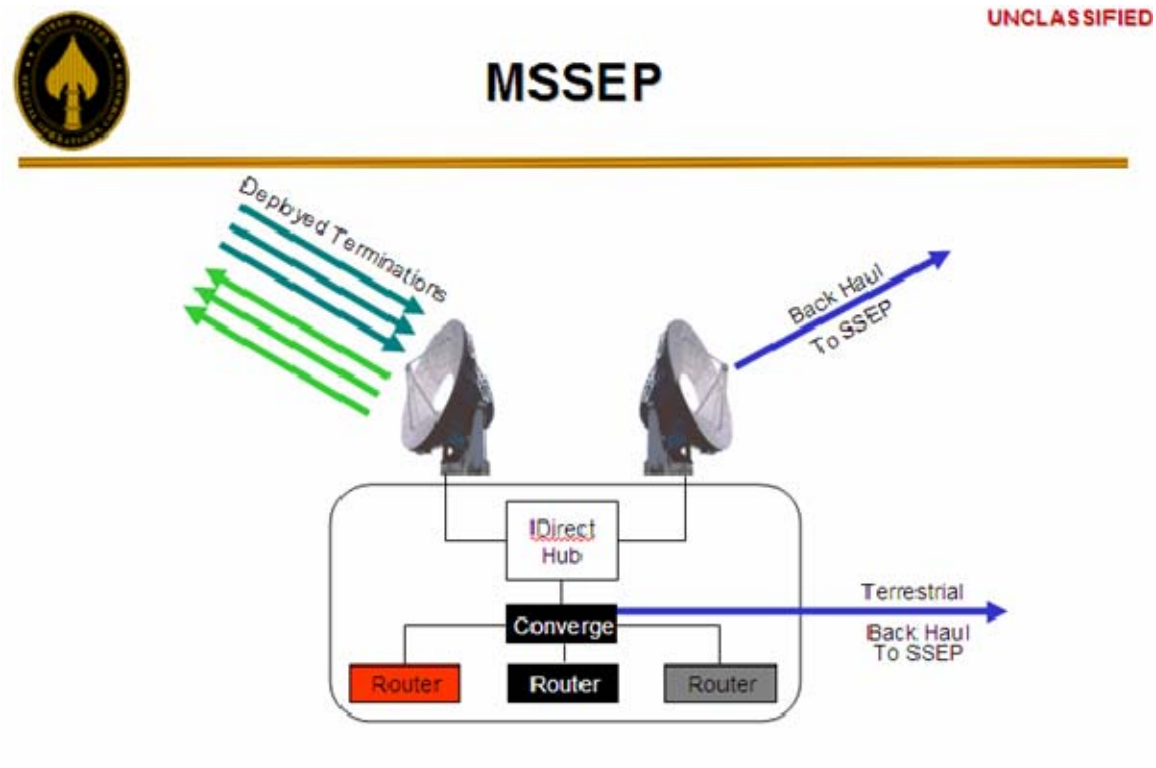

Figure 21. M-SSEP.

In the first case, the new M-SSEP will be designed to provide services locally for M-SSEP management. The gateway shall have full LAN (management of M-SSEP) and WAN system accreditations mirroring the existing SSEP. The operators will be able to manage the whole network in the area of operations without having to rely on the SSEP services. Thus, the Tactical Private Satellite Network that will be created for the purpose of a specific operation outside of the responsibility area of the existing SSEP will be entirely managed and integrated by the M-SSEP. For that reason, M-SSEP shall be designed so that deployed tactical users achieve "IP mobility" without system re-configuration — no matter where they enter the SIE.

For the second case, M-SSEPs shall be architected to provide connectivity to SSEPs and draw connectivity to services. It will augment the existing SSEP operations, but without providing services to local users apart from support of Red, Black, and Grey services for management and switching purposes only. Everything will

point to the SSEP. This is because the M-SSEP will bridge the different satellite footprints between the area of operations and the existing gateway with its two satellite dishes that will cover the two different spots. Figure 22 gives a picture of the above notion:

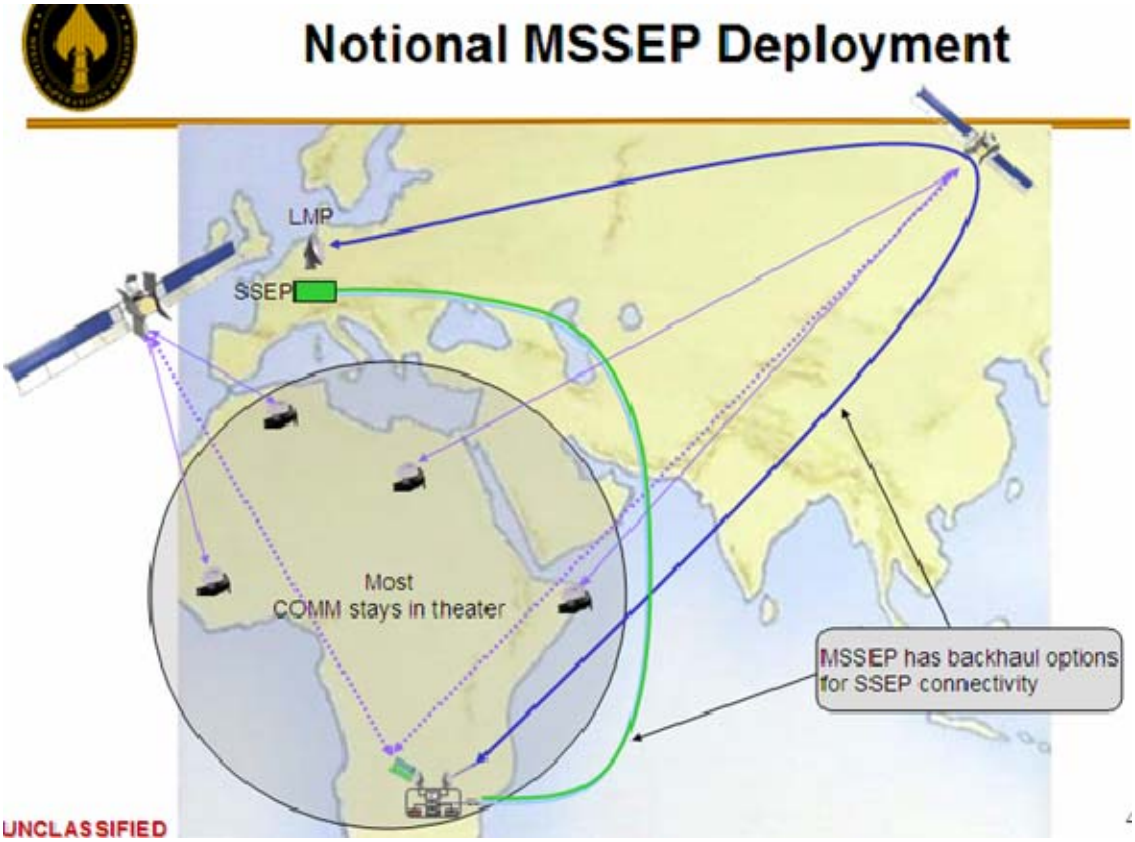

Figure 22. Notional MSSEP Deployment.

The whole M-SSEP configuration is complemented by the easy deployable size of the gateway which can be lifted by six persons maximum. In lieu of local power, when or where required, the power generation capability is capable of self sustained power generation.

The objectives need to be achieved without neglecting the risks — especially where human lives are involved. Given that the potential successful implementation of that mobile gateway can cause saturation of the available satellite bandwidth in specific areas, M-SSEP may absorb the satellite bandwidth and leave other

users in the area (who have not subscribed but who have equally importance missions) without communications and connections to command posts.

Another risk may involve the opposite result: over subscription of services at the SSEPs. Users may subscribe without having primary importance mission or they may ask for management services that may disorient the whole operation of the gateway. Due to the absence of a process for ordering, this may cause delays in responding to significant communication needs.

Last, apart from the need for clear specifications that exist, such as time schedules, funding, and training, so far there is a lack of defined services to support the operators who will maintain the M-SSEP when deployment is necessary.

As it can be easily perceived, the notion of M-SSEP project reflects and incorporates most of the attributes of a Tactical Private Satellite Network. It will be able to be deployed and to cover areas where the terrestrial infrastructure will be incompetent to cover the mission communication needs. It will act as the primary base station with full management capabilities without having the need to be physically in the imminent area of operations. This is because the collaborative satellite terminals will be there to re-establish communication. It must be in the same satellite footprint with one of its dishes. Further, by acting as a relay station with advanced capabilities and with the help of the other dishes which will be in the same satellite footprint with the permanent gateway, it will have the ability to pass the whole control to the existing permanent gateways.

The previously mentioned risks constitute areas of additional needed research for the correct implementation of M-SSEP. There is a potential “grey” area in cases where, in such a Tactical Private Satellite Network, non-military users need to subscribe to accomplish the mission. For M-SSEP, this is not the case. This is because its mission is clearly military-oriented, but, for the purpose of this research, a more flexible scheme with various level of confidentiality may need to be adopted. It is paramount to mention that M-SSEP will take under consideration the differentiations among different confidentialities (Black, Red, and Grey) so it may have the ability to be implemented when other governmental or NGOs participate in the operation. The final phase of

implementation of M-SSEP project, and its actual participation in the different operations, will reveal whether or not it is fully capable of forming and supporting Tactical Private Satellite Networks.

From the above two paradigms, it is shown that the notion of a Tactical Private Satellite Network, and how can be managed without the need of any terrestrial infrastructure, has been in a field of experiments for many years. The products of these experiments are at the point of accreditation and implementation in the operational fields. Connecting the dispersed units through satellite assets is no longer enough for conducting the operations. The capability to manage these communication lines is also paramount to guarantee complete and acceptable connections among the units and between them and the GIG.

Moving from the area of the conceptual requirements and design of a Tactical Private Satellite Network, the next chapter will examine the operational implementation of such a network in different situations, as relevant to its Tactical nature, and the contribution to the success of Net Centric Warfare operations. Different scenarios will be addressed and data of already conducted experiments will be cited to give understanding to its significance as an enabler of reliable and complete communication lines — either in dispersed military operations or in non-military missions where they are utilized during relief operations and are rapidly assembled to respond to ad hoc crises.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS FOR OPERATIONAL IMPLEMENTATION OF THE TACTICAL PRIVATE SATELLITE NETWORK

A. ANALYSIS FOR OPERATIONAL IMPLEMENTATION OF THE PRIVATE TACTICAL SATELLITE NETWORK IN SPECIFIC OPERATIONAL DOMAINS

Up to this point, the concept of a Tactical Private Satellite Network has been defined, examples of networks have been provided from both the civilian and military domain, and the desired attributes for this type of network was examined as well. The continuation of this study will include an examination of the operational application and implementation of a Tactical Private Satellite Network in four different domains. First, employment of a Tactical Private Satellite Network within the context of an experimental environment, specifically in the CENETIX at the U.S. Naval Postgraduate School and within the context of a MIO experiment, will be examined. Second, a conceptual application of the Tactical Private Satellite Network within the framework of maritime/naval operations will be examined. Third, an implementation in support of a ground combat application involving an evolutionary concept outlined the United States Marine Corps. Finally, an application of the Tactical Private Satellite network within the context of a Humanitarian Assistance/Disaster Relief (HADR) scenario where the military will operate with OGAs, NGOs, Coalition partners, and Private Volunteer Organizations (PVOs) will be considered.

1. Application of the Conceptual Framework of a Tactical Private Satellite Network in an Experimental Environment

The U.S. Naval Postgraduate School in Monterey, California, sponsors a CENETIX laboratory that focuses on the integration and networking of communications devices and sensors to create a shared network environment. A sub-set of the CENETIX functionality is the TNT, which is the physical network that CENETIX uses to conduct their experimentation. One of the major events run by CENETIX is the MIO experiments that test new operational concepts and devices (sensors and communications equipment) within the context of the MIO environment. Specifically, for the purpose of this section,

the MIO experiment conducted in March of 2008 will be the operational scenario that serves as the backdrop for the implementation and application of the Tactical Private Satellite Network in an experimental environment. The integration of the Tactical Private Satellite Network into the CENETIX lab and the TNT network will be examined in further detail later in this chapter.

According to the final report issued by the CENETIX lab, the MIO 08-2 experiment continues to build upon previous experiments to evaluate the use of networks, advanced sensors, and collaborative technology for rapid execution of MIO. Specifics include the ability for a Boarding Party to rapidly set up communications that facilitate the search for contraband — namely explosive or radiological material — as well as physical characteristics of target vessel crew members. Additionally, the maintenance of network connectivity with C2 organizations and collaborating with remotely located sensor experts, with the specific goal of exploring new sensor, networking, and situational awareness solutions for tagging, monitoring, and interdicting small craft, threatening the security of the coastal metropolitan areas (MIO 08-2 Final Report 16) are included.

In general, the goal of the TNT network is to maximize information sharing between Boarding Parties and the Tactical Operations Centers (TOC) which serve as the major C2 nodes. The TNT network topology, depicted in Figure 23, consists of varied communications technologies that facilitate the information sharing between C2 nodes required by the operators conducting operations. The primary long haul means is done by numerous 802.16 WiMax Orthogonal Frequency Division Multiplexing (OFDM) links that connect the major C2 nodes, and serves as a transport for the smaller bandwidth mesh networking technologies that are used by the Boarding Parties during the operations.

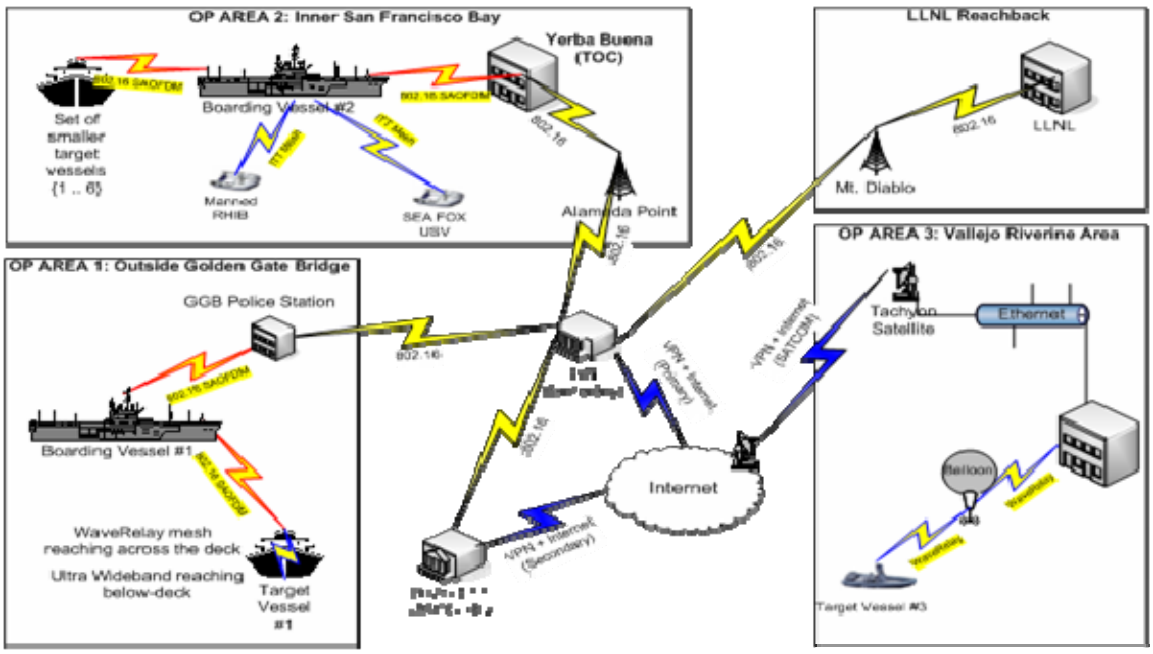

Figure 23. Overview of MIO 08-2 Communications Architecture (from MIO 0802 Final Report).

In addition to the physical communications architecture, the TNT network that supports the MIO consists of a VPN that connects various entities within a secure environment by providing end to end encryption. This allows the TNT network to utilize public infrastructure. The following figure illustrates the VPN architecture utilized during MIO 08-2:

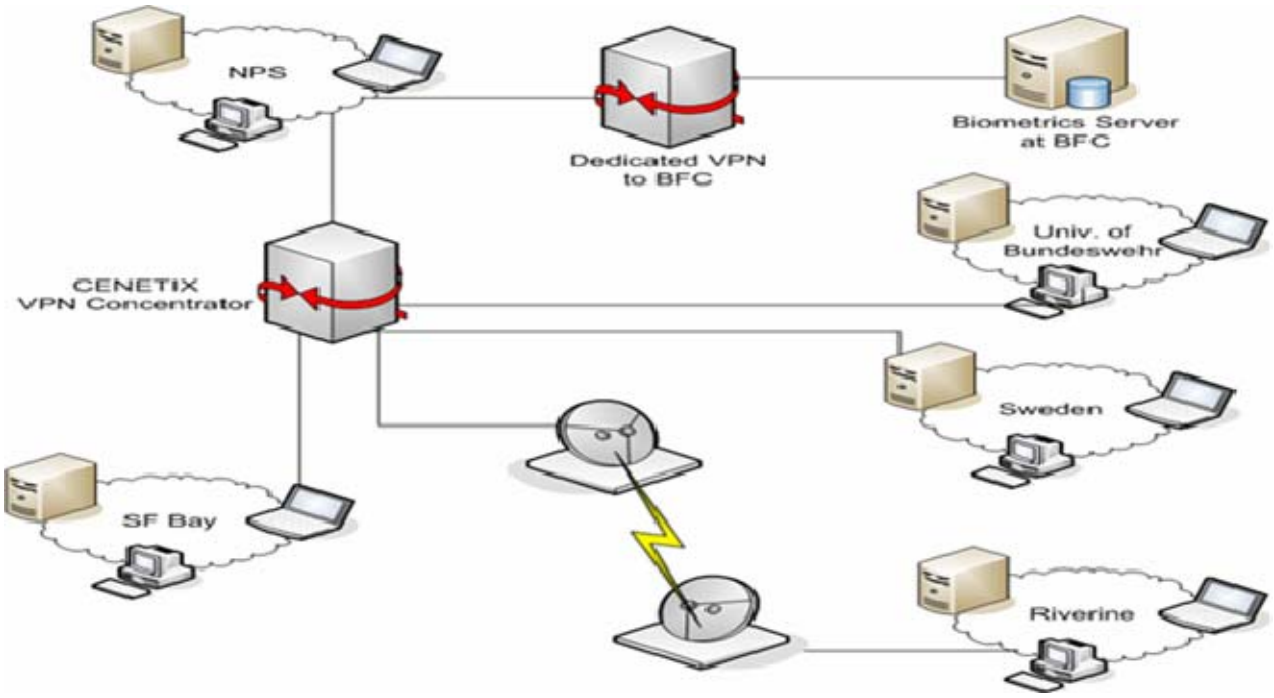

Figure 24. MIO Domestic and International Reach-Back Network Topology.

Beyond the existing OFDM network, a satellite link was established for the purposes of experimentation and integration to take advantage of VSAT equipment that was procured by the CENETIX lab for said purposes. The equipment that was procured was the Swe-Dish IPT suitcase VSAT terminal. It is, hence, referenced as IPT. Initially, the operational configuration, as seen in Figure 25, was the initial plan for the experiment and was designed to provide access to Internet resources via commercial satellites as a redundant link to OFDM network. Support was received by the Swe-Dish IPT manufacturer for training of personnel on the operation of the terminal as well as the acquisition of satellite air time for the duration of the experiment.

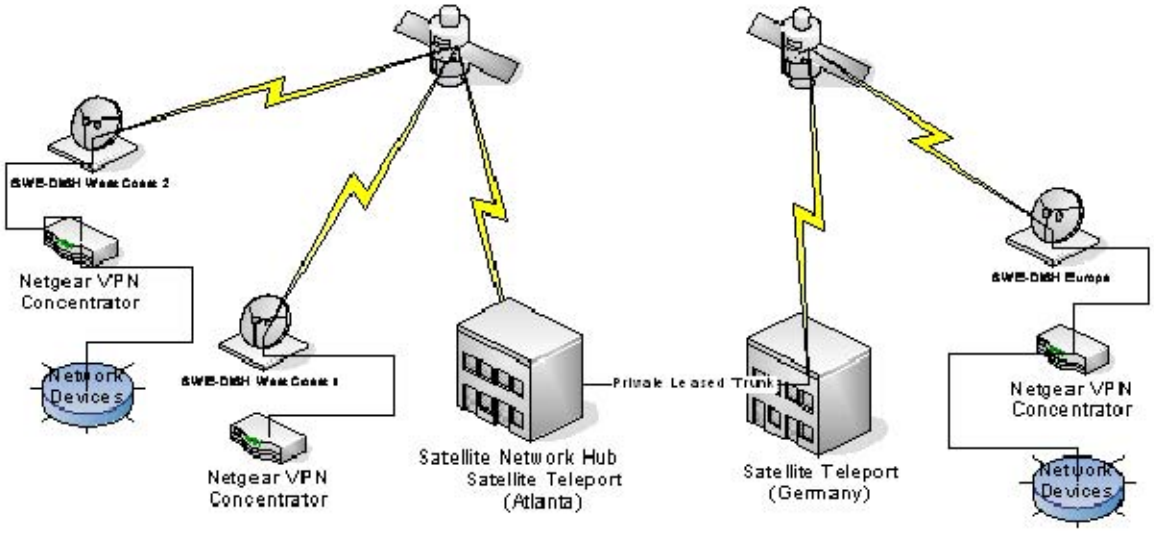

Figure 25. Original Swe-Dish Architecture.

Because of the geographic dispersion of the satellite terminals during the experiment (one in Europe and two in the U.S.), a commercial ground station was planned to act as an intermediary between Internet services and the satellite terminals. For the two terminals in the San Francisco bay area, no ground station was needed because both were planned to work with the same satellite. The satellite that was used as the connection between the two nodes in California was the Galaxy 10R satellite. The Galaxy 10R satellite, launched in January 2000, is a telecommunications satellite located at 123 degrees west in geostationary orbit and operates in the C and Ku Frequency bands that provide coverage to North America (Satellite Fact Sheet; Galaxy 10R). Figure 26 provides a graphic representation of the location of the Galaxy 10R satellite with relation to the MIO Operating Area:

Figure 26. Location of Galaxy 10R Satellite (from http://www.n2yo.com/ ?s=26056).

This backbone was designed to provide Internet access and reach-back capability for the various elements participating — either in the U.S. or abroad. Since the terminals could have provided reach-back on the TNT network, via a VPN connection, it was expected that the participating terminals could be monitored from a remote location, such as the NPS Network Operations Center (NOC).

Since the IPTs had not been deployed within the context of this experimental environment previous to this, the particular management capabilities of the resident modem could not have been ascertained due to limited information on the new hardware. Discussions with the vendor were conducted to ascertain user management capability and rights. The critical factor pertaining to the IPT was the performance of the modem across the satellite link – remembering that there are several hops involved (through the ground station and into the public Internet) before reaching the other terminal. Within the context of system performance, it was desired to determine the amount of packets transmitted,

packets received, and packets lost across the length of the link (from terminal to terminal) since no more information, due to its proprietary nature, has been obtained about the capabilities of the embedded modem. The injection of this new system into the TNT network warranted study and consideration of performance on an active network with various types of traffic being transmitted. Until the beginning of the experiment, limited information had been received concerning the capabilities of the embedded modem and its compatibility with the current solution of SolarWinds (the primary network management tool utilized by the NPS NOC). This test had been conducted in a hospitable environment under optimal conditions. No matter how good the system performance matched the capability claimed, it is still recommended that further testing be conducted in other more realistic operational scenarios and under adverse environmental conditions. The finalized network architecture for the California portion of the MIO is illustrated in Figure 27:

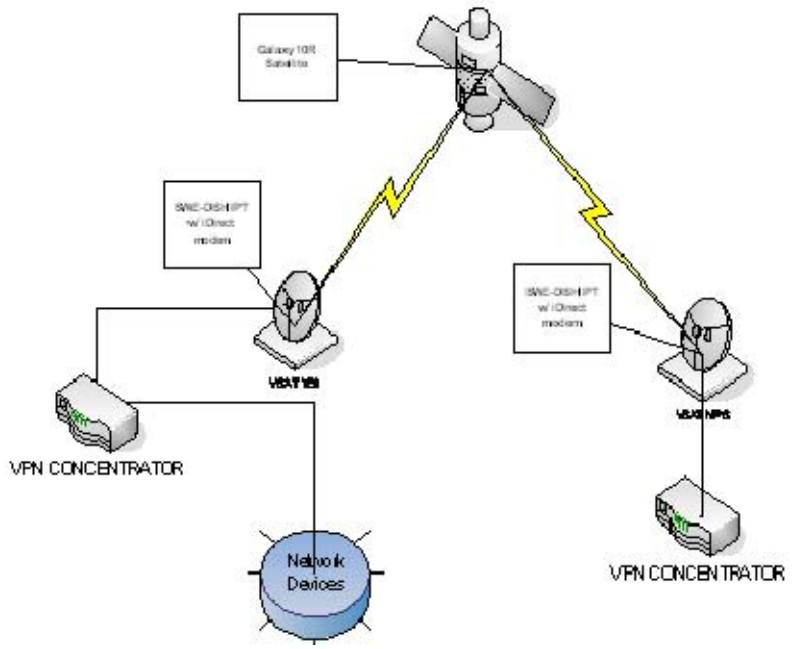

Figure 27. Final IPT Satellite Communications Architecture in Support of MIO 08-2 (from MIO 08-2 Final Report).

The connection with the Yerba Buena Island (YBI) IPT and the NOC were completed to observe the whole operation remotely from the CENETIX lab. Figure 28 illustrates the initial set up of the nodes through the proprietary software of the provider (iSite).

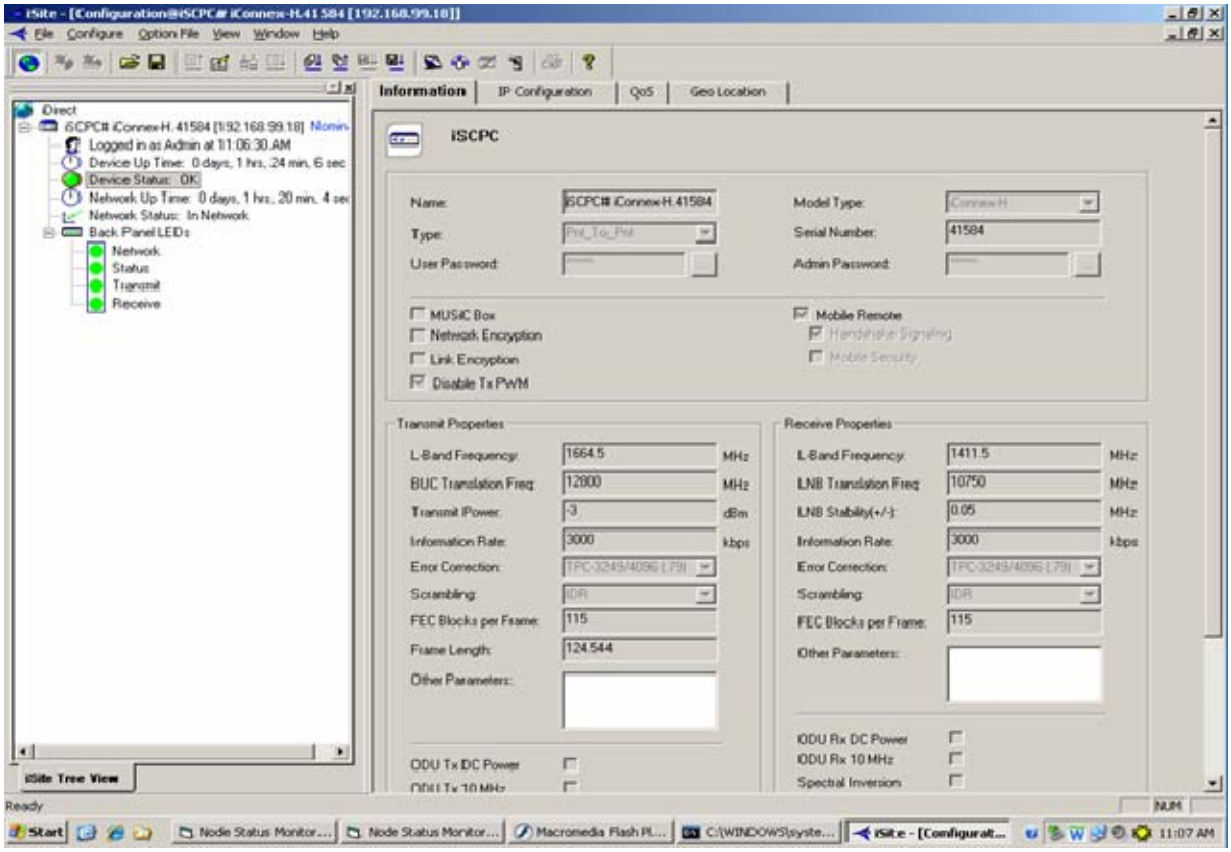

Figure 28. Initial iSite Set up between NPS and YBI.

From that specific software application, the ability was provided to monitor the performance of every node on the network by soliciting information by IP address of the modem.

A fortunate mishap changed the initial scenario: the primary OFDM backbone failed during the height of the experiment. Therefore, the communications fell back to the designated backup link established between the IPTs. Figure 29 illustrates the restoration of transmission through the IPTs from the SolarWinds management console:

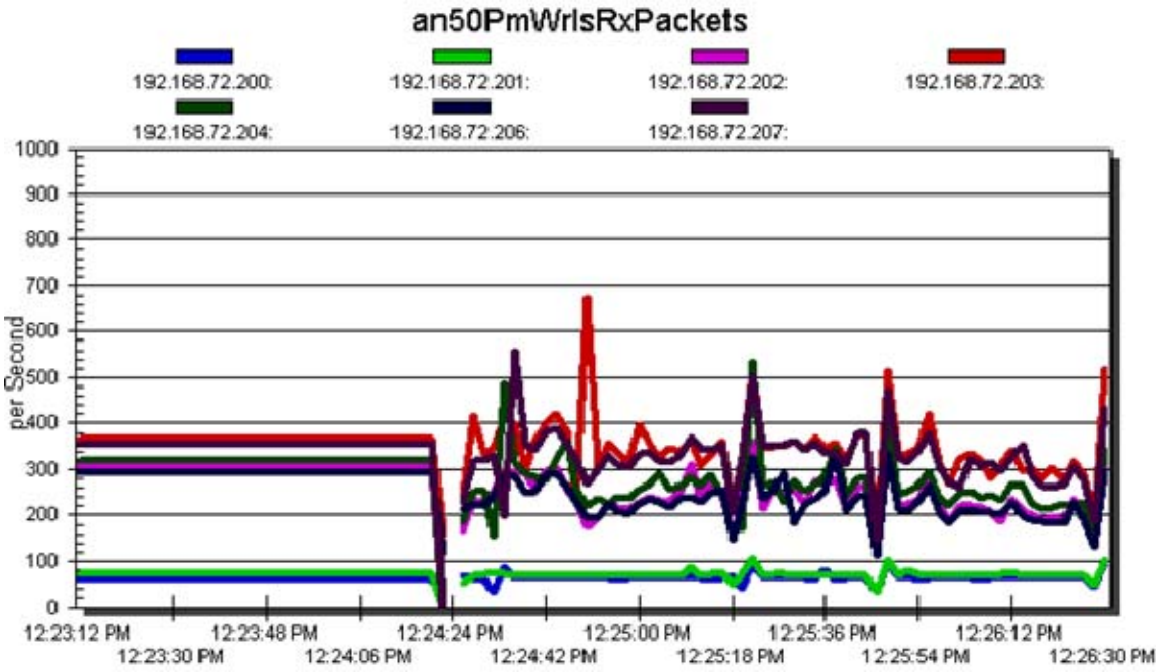

Figure 29. Swe-Dish Takes over the Transmissions.

Though the proprietary software, iSite monitoring of the throughput from both nodes (YBI and NPS), in terms of transmitting and receiving for a number of different packets (UDP, TCP, ICMP, IGMP, and HTTP) and the total one, was possible. Figures 30 and 31 illustrate different time instances of monitoring the performance of IPT through the proprietary software. The upper node depicts YBI which is the one that was continually monitored as it was the only one that kept sending packets. The other node is the NPS NOC. The upper right screen illustrates what was being transmitted and the lower right one what was being received. As is easily shown, the vertical axis illustrates the speed of transmission/reception and the horizontal one shows the respective time instance. The different color lines illustrate the different packets that were traveling across the network at any given time. From the satellite provider, it was known that for the specific service a three MB pipe had been available. During the whole participation of the IPT, and according to collected logs, a 2.53 MB/sec speed of transmission had been achieved.

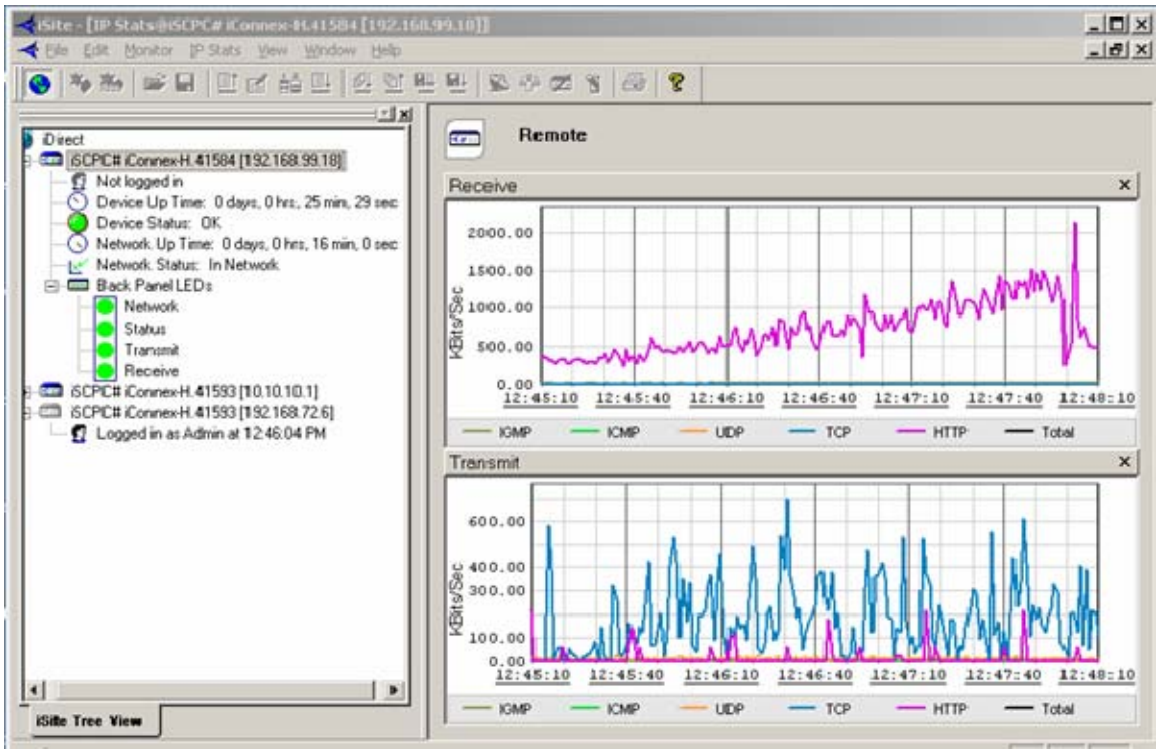

Figure 30. Web pages, GOOGLE Earth File and Groove are Going over.

Figure 31. Observations of Swe-Dish Performance.

Moreover, QoS for each type was also monitored. Figures 32 and 33 illustrate the QoS for each packet for the modem 192.168.99.18 (YBI) and 192.168.72.6 (NPS):

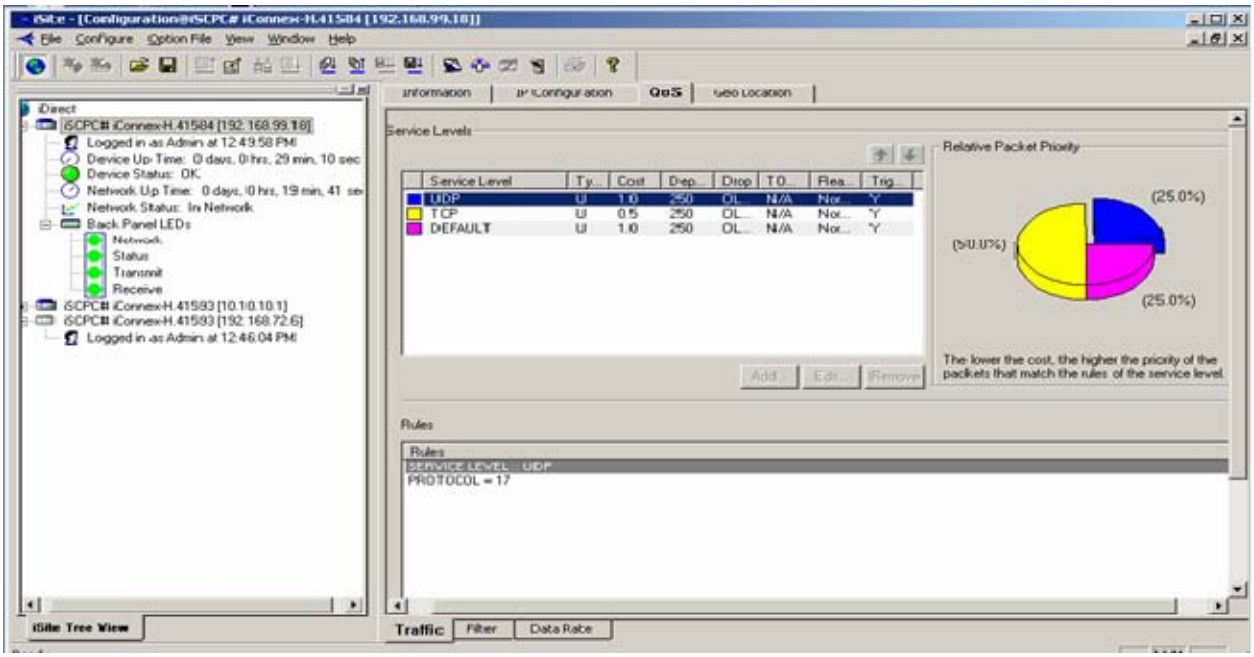

Figure 32. QoS for YBI Modem.

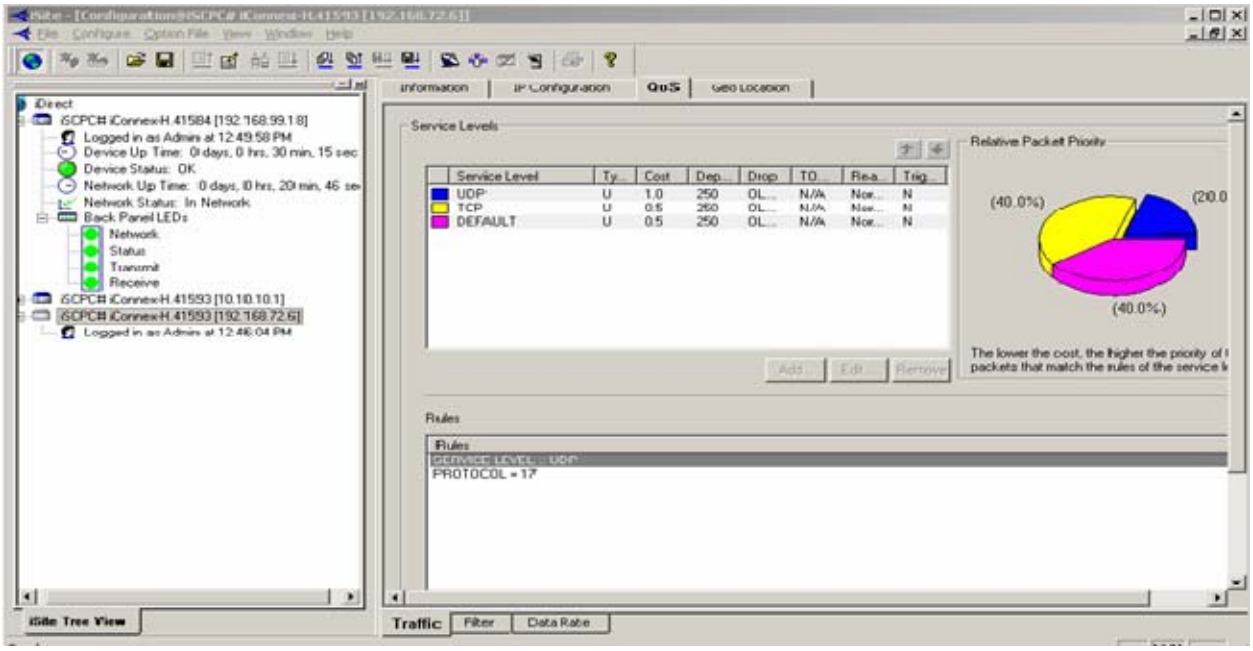

Figure 33. QoS for NPS Modem.

The above QoS parameters that are displayed on the iSite software are defined in accordance with the software developer's use parameters, which were kept proprietary by the manufacturer. Figure 34 illustrates that transmission over the IPTs had been shut down. The overall performance of the two IPTs was commented as satisfactory and no problem in transmission was reported:

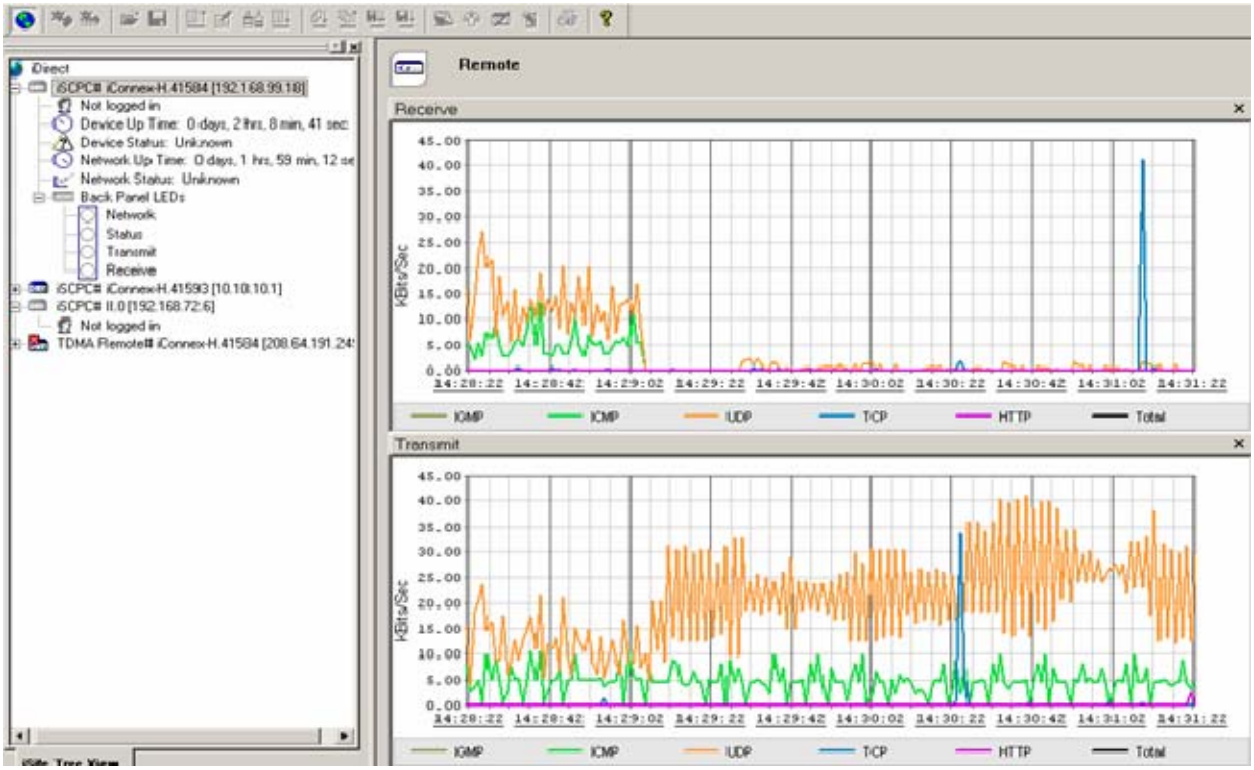

Figure 34. Shutting down of Transmissions: 14:29 (12 March 2008).

The above experiment utilized only two VSATs and the services provided by the IPT manufacturer. Still, it demonstrated the major benefits that satellite communications can bring to the experimentation field. It had less specific measurements than a complete experiment because experiments additionally involve establishing some level of control and also manipulating one or more factors of interest to establish or track cause and effect (Alberts and Hayes, Codes of Best Practice experimentation, 19). Even acting as a "sidekick" of the OFDM backbone and with the constrained abilities to only monitor

(measure) the overall operation of the network, the two VSATs managed to undertake successfully the whole volume of the communications. They dynamically formed an ad hoc network which consisted of these two terminals and, at the same time, with their proprietary software, provide the operators at both ends with a clear picture of that network's properties. SolarWinds completed the picture for the rest of the nodes which participated as if nothing has happened to the primarily OFDM backbone. By moving few steps ahead, the complete implementation of the Tactical Private Satellite Network would facilitate further experimentation in two important ways. First, the Tactical Private Satellite Network will provide an alternate communications path that can be used to connect different experimentation sites and serve, as seen in the MIO case study presented previously, as a redundant communications link. Additionally, if experimentation sites are located within the same satellite footprint, such as locations within same continent (i.e., New York and California), then the satellite network can expand the overall reach of the test network and allow for the inclusion of more sites in different locations. The Tactical Private Satellite Network can also expand the ability to incorporate different types of platforms into the test network. For instance, the proper implementation and integration of this satellite network aboard surface naval vessels and other watercraft that would normally operate out of range of traditional LOS transmission means would serve to enable a variety of different types of experiments that would ultimately provide a more robust test and experimentation network.

The second way in which the implementation of the Tactical Private Satellite Network would benefit the experimental community is that, due to the ever-increasing amount of satellite communications that is being utilized by the military and other governmental agencies, the satellite network would provide a ready network for users with a "plug and play" capability. This would happen in much the same way that the OFDM network already employed by the CENETIX/TNT lab provides to experimentation today. Therefore, specific applications and information exchange requirements that are identified to be met by satellite communications can be tested on a real-time satellite network. Other issues relating to the satellite-based networks — network management, performance of networking protocols, specific hardware and

software applications, and associated issues — can be tested in an environment that would provide more accurate information. Test results could then be obtained by simulation alone.

During the events associated with the CENETIX MIO 08-2 experiment, it was proven that commercially available VSATs are capable of handling the amount and types of traffic that would be found on the modern battlefield. The IPTs that were employed during the MIO successfully transmitted a variety of TCP/IP-related traffic through a commercial communication satellite in geostationary orbit with little to no degradation in service noticed by the users. The proprietary software that was included with the terminals allowed network managers to view the performance characteristics of modems embedded in the other terminals on the network. Managers, however, are limited to viewing performance and are left with no ability to remotely conduct troubleshooting or remote manipulation of the operating parameters of the modems. The network managers were able to use a commercial product, SolarWinds, to view the types of traffic traversing the network and use those statistics to make informed decisions with regard to the health of the satellite link. Ultimately, a desired quality of the Tactical Private Satellite Network is for the NECOS that is operating the network base station to have the ability to remotely manage and view the performance of the embedded modems. It is also desirable that the network managers and operators have the ability to remotely manage the network devices that are located off of subordinate terminals within the same domain/network. This remote management will be explored in greater detail in Chapter V.

In summary, the implementation of the satellite communications network during MIO 08-2 utilizing the Swe-Dish IPT VSAT proved that the basic concept of the Tactical Private Satellite Network is viable — not only from an operational perspective, but also from the perspective of an experimentation and test environment. The employment of this network has illustrated advantages and limitations of such system, but the overall result has been positive. There are presently some issues relating to the management of the actual iDirect modem that is embedded within the terminal, but other methods of management can be used to address the network components that are directly connected to the satellite dish. The implementation of the Tactical Private Satellite Network within

the context of the CENETIX/TNT network would serve to provide a more robust communications environment and facilitate the test and evaluation of current and future applications and satellite communications-related research.

Considering that the concept of the Tactical Private Satellite Network has been implemented, tested, and proven in laboratory environment, the following sections will examine the implementation and integration of the Tactical Private Satellite Network within different operational scenarios. The scenarios that will be examined are a maritime case, the operational implementation within the United States Marine Corps, specifically the SCMAGTF, within the context of a coalition environment, and, finally, how the Tactical Private Satellite Network facilitates Network Centric Operations will also explored.

2. Analysis for Implementation and Application of Tactical Private Satellite Networks in the Maritime Domain

One area that most benefited from the implementation of a Tactical Private Satellite Network is the maritime domain, where satellite communications is a widely used commonality. It would be trivial and out of the scope of this research to analyze the reasons behind using satellite communications aboard naval vessels operating all over the world. More or less, maritime units can resemble dispersed ground units or generally mobile nodes operating far away from their base. Back in 1959, Chief of Naval Operations, Admiral Arleigh A. Burke, had already recognized the value of satellite communications and wrote a memo to fleet commanders saying: "The use of satellites for naval purposes is going to come about in a few years: the necessity for close coordination of things pertaining to space with other naval functions will become increasingly important"(Burke). Today, with the shifting of the Navy to a net centric environment, Admiral Burke's direction is equally relevant.

In such an increasingly complex environment as the one that Navy operates there is a great demand for speed of decision and precision together with persistence in action. Assured access to space capabilities will give decision-makers the advantages of speed and persistence to respond to the full range of military operations. For that reason, net

centric operations rely on satellites as the communication backbone to integrate huge volumes of data from widely dispersed decision makers.

While there is wide usage of satellite capabilities in the global maritime domain in terms of communication and accurate positioning systems, there are even more in the Navy operational domain where space capabilities, such as satellite communications, ISR, Global Positioning System, and missile warnings are the backbone of the modern operational net centric environment. Especially for operations at sea, often SATCOM is the only way to provide reliable, global communications in a timely manner. Apart from the profound lack of terrestrial infrastructure and the highly mobile nature of naval operations, the rest of available means of communications have inherent limitations: high frequency radio lacks the reliability and the capacity required for military operations and line of sight radios have neither the range required nor the ability to operate in all topographical areas. To that direction, naval operations either independently, or as a part of Joint operations, have included the concept of being connected with the other assets — terrestrial, aerial, and maritime — through commercial or military satellites as depicted in Figures 35 and 36:

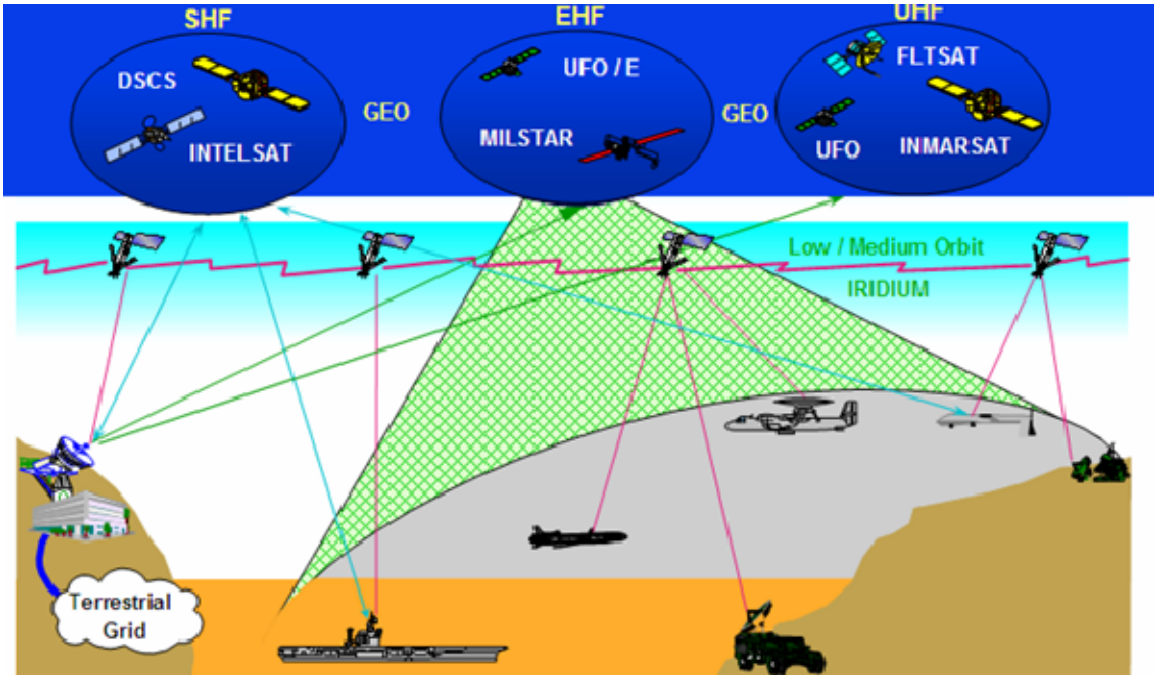

Figure 35. Satellite Communications in Joint Operations.

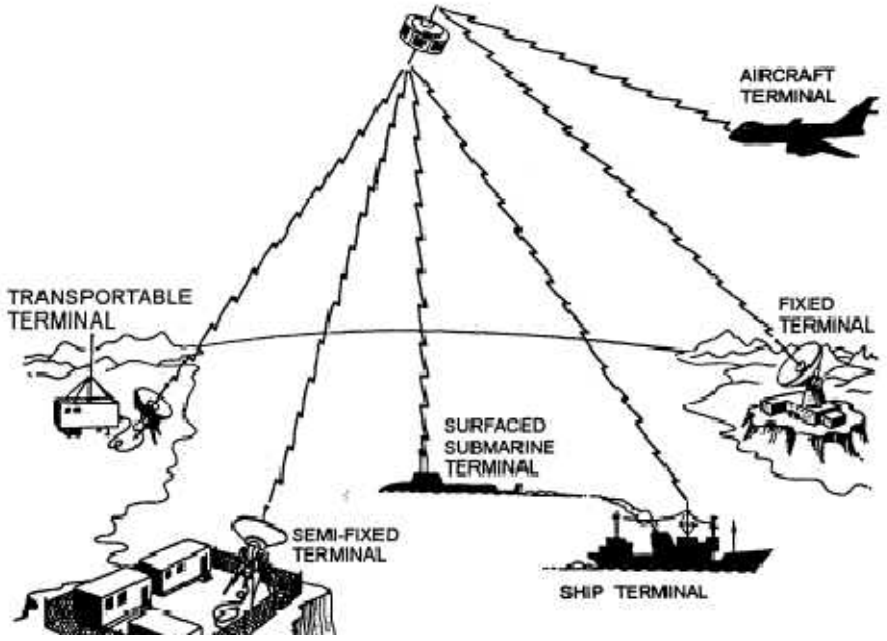

Figure 36. Satellite Communications in Pure Maritime Environment.

Especially in terms of using commercial satellites, naval operations and the whole maritime community have been provided with good communications links to ships at sea. Satellite communication systems, such as Inmarsat, Iridium, and Intelsat have been leasing their services by connecting their proprietary GEO or LEO satellites to the ships. Links, using their on-board compatible VSAT type devices, connect the ship to a land-based point of presence to the respective nation's telecommunications system. Figure 37 depicts the topography of Challenge Athena. This is a project of Intelsat to provide communications to large ships having large antennas, large bandwidth, Internet/Sailor phones, and two-way communications:

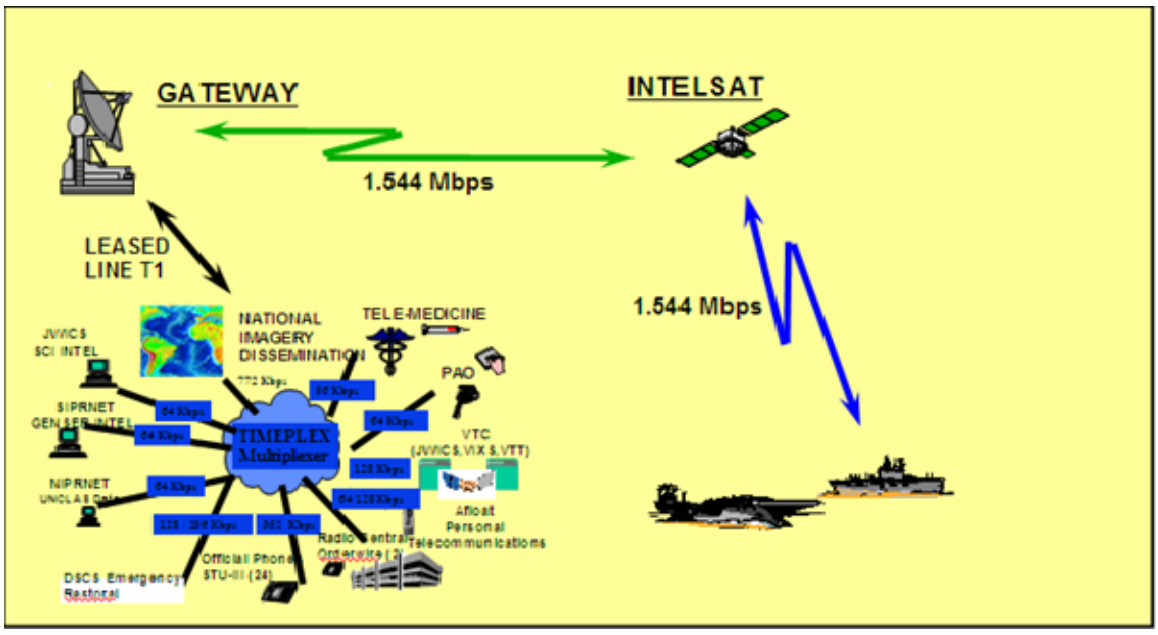

Figure 37. Challenge Athena Topography.

Of course, in the above commercial-based implementations, the vessels participate in a Satellite Network without the capability to manage it. They cannot detect and repair potential failures or guarantee QoS. The sole users' interaction with the network is the initial leasing of the required lines. Management functionalities remain on the contractor side that is responsible for the overall operation of the network.

As in all the other military operations, the mobility and time constraints of the naval operations, along with the security implications, would require a more independent type of management for the network inside the allocated bandwidth framework from the contractor. To that direction, naval operations would benefit from the implementation of a Tactical Private Satellite Network for more optimum utilization and management of the satellites resources that would have been assigned for a specific mission. The following paragraph refers to a very generic — and by no means exclusive — scenario of naval operations where the merits of a Tactical Private Satellite Network are demonstrated when satellite communications are the only means of information dissemination among the vessels. The vessels conduct and the ground headquarters supervise and coordinate the specific mission.

a. Description of the Scenario: "Sailing Overseas"

Naval vessels have often been characterized as a powerful means of diplomacy around the globe. This is especially true today: naval forces have been called to undertake missions in every sea corner of the world to enforce UN regulations for the peace and prosperity of all nations. Consequently, it is not unusual for large battle groups, formed by allied forces, to operate in areas where either there is no infrastructure in the mainland or it is not available. In these areas, the naval vessels are required to conduct a great number of — defensive or offensive — missions without having the luxury of nearby headquarters or land communication facilities to transmit, receive, and disseminate information that is critical to operational flexibility or to global awareness. Furthermore, for the sake of other operational areas, the saturation of military bandwidth may also deprive them of relying upon military secured and guaranteed proprietary satellite networks. For that purpose, the implementation of a commercial satellite to satisfy the communication needs of such a naval force is crucial. The overall capability of managing it can further benefit the conduction of the mission.

A proposed scenario of the naval operation dictates that the battle group is deployed: to conduct MIO operations 20 miles away off the coastal line of X country with a very unstable government where civil war is taking place and the human rights of the citizens are being violated. The ultimate purpose of the mission is to forbid vessels with dangerous cargos (guns of any kind) to penetrate the sea line of surveillance and hand them to adversaries on either side; food supplies and medical provisions of any kind are to be directed to specific ports of a nearby country for accurate enumeration and proper dissemination to the UN representatives.

As easily understood, an overt mission, such as the above, requires a great deal of information and knowledge flow from the battle group to the directive headquarters, and vice versa, to guarantee a clear operational picture of both sides. The headquarters needs an accurate naval picture of what "sails" in the assigned territory and what actions have been taken to divert vessels or to conduct boarding operations on them. Eventually, the headquarters needs an accurate picture of every vessel sailing in the area with its proper classification. On the other hand, the battle group commander needs real-

time information for what to expect in the area. The commander also needs fast responses to his inquiries about the documentation of the Contacts of Interest (COI) which the ships challenge to identify them.

Such dual directional lines of communications do not suffice with voice data. Pictures and documents need to be disseminated. There needs to be collaboration with other civilian authorities, such as port captains or companies' representatives, to establish and deliver proper clarifications to all sides. For the UN and military participants, time means lives. For the companies that own the ships, time also means money. Implementing a robust satellite network, in the form of a Tactical Private Satellite Network with the capability of proper management, seems an ideal — if not the only — solution for the overall success of the operation.

b. Depiction of the Application and Benefits of Implementing the Tactical Private Satellite Network within the Context of the MIO Environment

Such an ad hoc and extremely mobile network can easily take on the definition of a Tactical Private Satellite Network. A mobile base station with control and management capabilities on the network can bridge the gap between the dispersed naval units and provide the global awareness, operational flexibility, and information exchange required. It can help in the procedure of taking real-time decisions and dynamically reposition the units on the sea terrain. It can further allow the unscheduled addition of terrestrial nodes, such as the nearby country's station, in the network without degradation of the overall performance or problems in the authorization of the additional nodes.

This empowered base station, which resembles the above M-SSEP, can act as a hub to the linked network. If this work gives the modularity of Barabasi (Barabasi, 230) to this experiment's battle group and cluster of nodes, then the hub (base station) can link this module with the rest of the communication world —in this case, potentially the GIG — and establish a well-connected network with scale-free topology attributes (Barabasi, 87). This CGW can be stationed either aboard the command ship or ashore at the nearest friendly country.

In the first case of being placed aboard the command ship, the satellite footprint can easily cover a large area — enough to include friendly territories where their terrestrial infrastructure can be used for further connection to the GIG. Depending on where the area of operations is, the footprint can also cover alliance's major telecommunication centers which can complete the dissemination.

In the second case, as mentioned above, because of the size of its satellite footprint, the coverage of the sea area of operations will not be a problem — even if the nearest land is 200 miles away. Thus, the mobile ground station (or CGW) will be able to operate and, simultaneously, be secure from adversaries' hostilities. From there, the existing terrestrial infrastructure will undertake the burden of integrating the communication lines and completing the loops.

In any of the above cases, and for the sake of survivability of that network, a secondary hub will be needed to guarantee the scale-free topology of the proposed network. Consequently, in the case of removing the primary hub, the linked network will not collapse. The role of a secondary hub can be undertaken by the ground station or the command ship when they do not have the role of the primary hub. Moreover, the major units — maritime or terrestrial — must be equipped with VSATs to complete the Tactical Private Satellite Network.

The overall management of the network, though centralized from the base station, can further adopt a hybrid form by decentralizing sub modules and deploying smart agents to collect the data from the managed objects and report to the base stations. This simulates Remote Monitoring (RMON) functionality.

The proposed connectivity without any technical specifications is depicted below in Figure 38. On the figure potential CGWs have been identified and noted and possible communication lines (satellite or not) have been drawn. The design is by no means exclusive; rather, it represents potential connections for the given scenario.

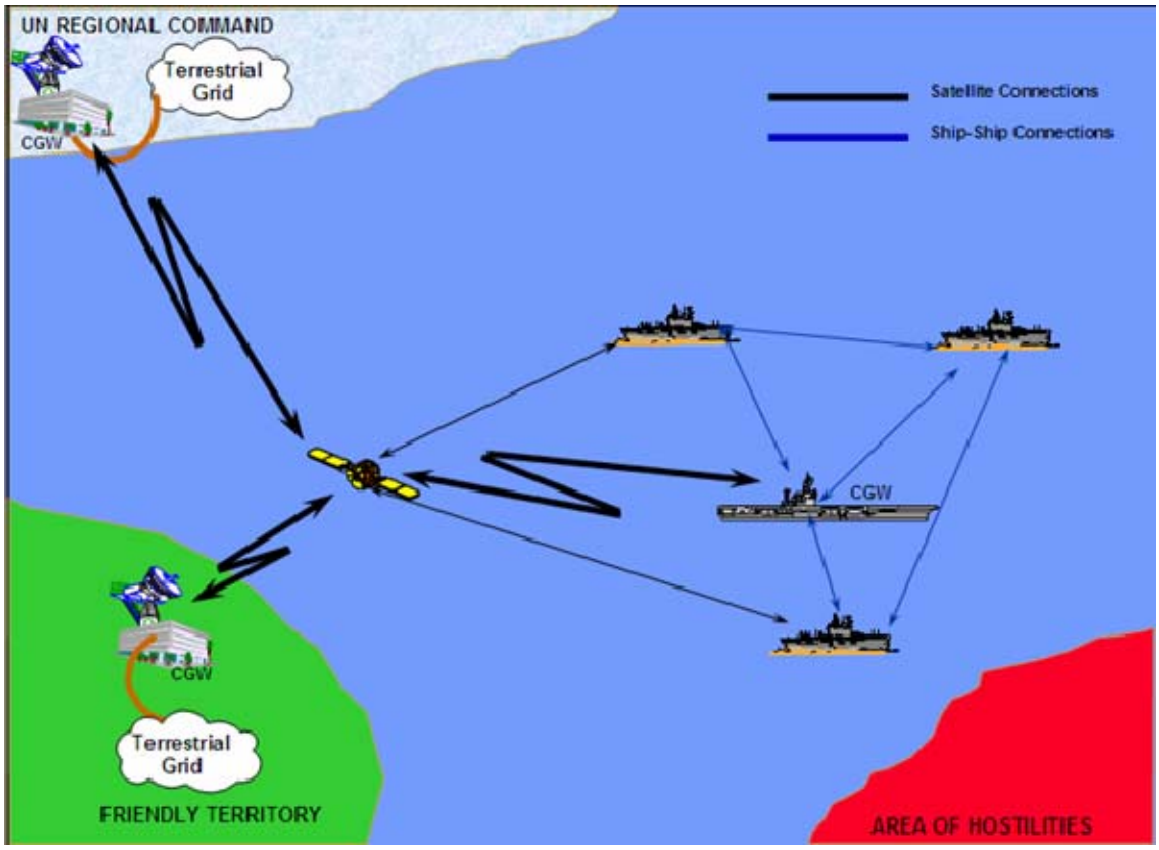

Figure 38. Maritime MIO Scenario.

Such self-dependent connectivity will bring a number of benefits to the mission through the abrupt communications lines among the participants. It will give the network the overall flexibility of self-managing and self-forming within the assigned boundaries of the allocated bandwidth. Inside these boundaries, the network manager can allocate the bandwidth to the individual units in accordance with their specific needs.

Furthermore, collaborations tools will be deployed on a controlled basis so as not to consume valuable bandwidth during critical time windows. Faults inside the network can be tracked and repaired in a timelier manner rather than relying on a provider with multiple priorities. Managers and agents will be deployed in accordance with the specific needs of the network and aimed at specific components of QoS.

As mentioned above, on the tactical level, because of fast and accurate exchange of information, timely decisions will be made. Knowledge from experts will be

recruited from other continents for the benefit of the mission. Headquarters and on-scene units will share the same tactical picture and acquire SA at all levels.

In conclusion, the overall product will be a well-designed Net Centric flavor mission. It will not only send accurate pictures to headquarters, but it will properly distribute the power to the Edge (in this case, to the battle group commander). The robustness of the network will give him the assurance of connectivity with all levels. It will let him make decisions on an operational level free from any communication constraints. It will further assist him by pulling the proper information when needed rather than waiting for an abundance of data — relevant or not — to be pushed at him.

3. Application of the Conceptual Framework of a Tactical Private Satellite Network in the Context of the United States Marine Corps Security Cooperation MAGTF

The third operational implementation of the Tactical Private Satellite Network that will be examined is within the context of the newly established operational concept for the United States Marine Corps — the SC MAGTF. The concept of the SC MAGTF was brought forth by Headquarters, U.S. Marine Corps in January 2008. According to this new doctrine, the Marine Corps' new operational concept is focused toward the establishment of a global, persistent forward presence tailored to build and enhance security while adapting the existing force structure and creating new capabilities (Headquarters, U.S. Marine Corps 6). The creation of this operating concept, and the genesis of the SC MAGTF, provides an excellent opportunity to overlay the architecture of the Tactical Private Satellite Network onto this new operational concept. The SC MAGTF will provide the regional Combatant Commander with a flexible expeditionary force that will serve to further augment existing Marine Corps capabilities (Headquarters, U.S. Marine Corps 18). Therefore, it is crucial to understand the operational concept and the support that the Tactical Private Satellite Network provides.

For the purposes of this examination, the following scenario is illustrated. The SC MAGTF is deployed to varied locations on the African continent providing a forward presence and engaging in variety of mission profiles. Figure 39 illustrates the operational dispersion of the SC MAGTF. Specifically, the headquarters of the SC MAGTF

is located, with subordinate units, in Rota, Spain. For the purpose of this example these are located in Ghana, Nigeria, and Kenya.

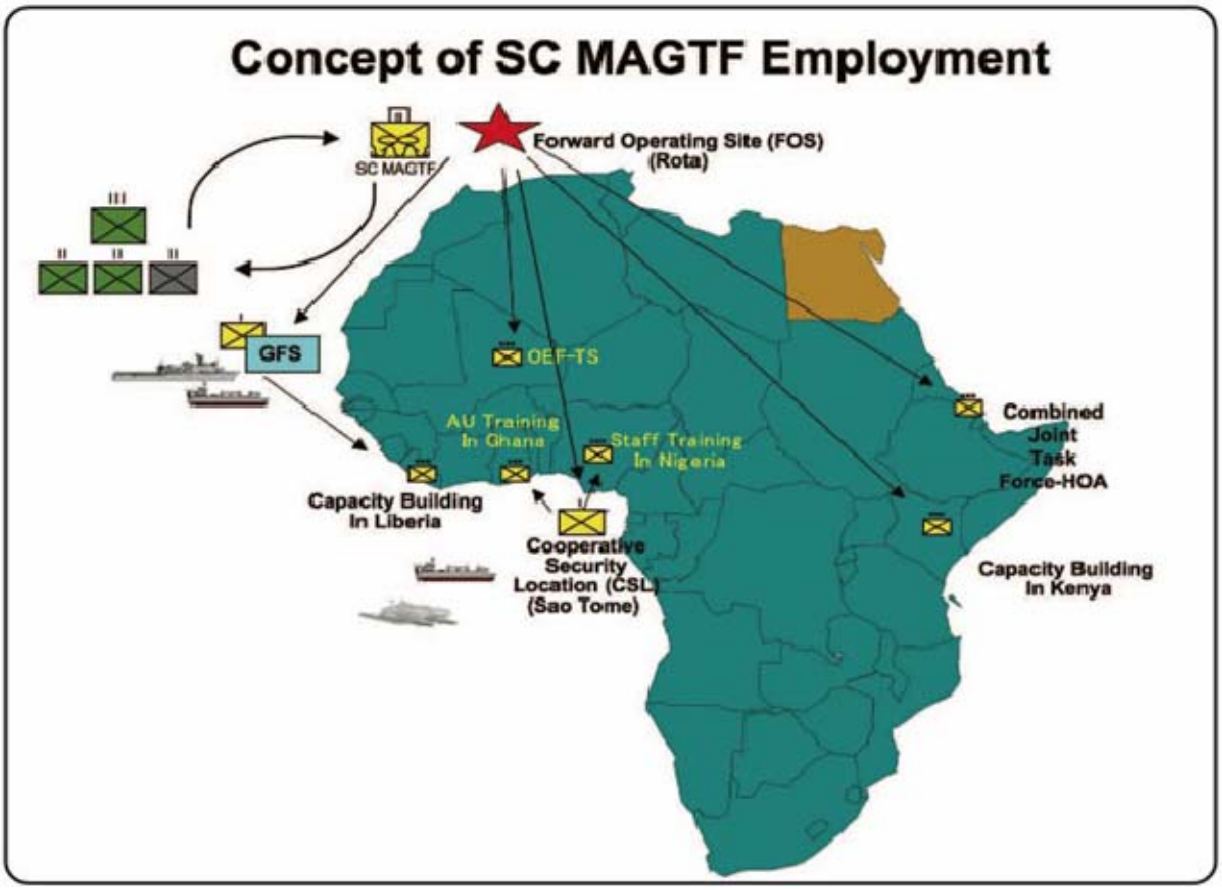

Figure 39. Concept of SC MAGTF Employment (from http://www.marine-corps-association.com/gazette/jun08_fighting_the_long_war.asp).

One of the methods crucial for the success of SC MAGTF operations is that the elements of the SC MAGTF are globally connected. These forward operating Marine units that are operating in remote locations will require a robust information system that will transmit, receive, and disseminate information critical to global awareness and operational flexibility (Headquarter, U.S. Marine Corps, 32). The implementation of the Tactical Private Satellite Network can bridge the gap between the headquarters element and the dispersed units. It also can provide the global awareness, operational flexibility,

and information exchange required. The hub, or base station, for the Tactical Private Satellite Network would be located where the SC MAGTF headquarters is located. For this illustration in Rota, Spain, and the subordinate units deployed to Ghana, Nigeria, and Kenya (as outlined in the operational concept) employment would be compatible to VSAT terminals. A sample architecture that would support the SC MAGTF is illustrated in Figure 40:

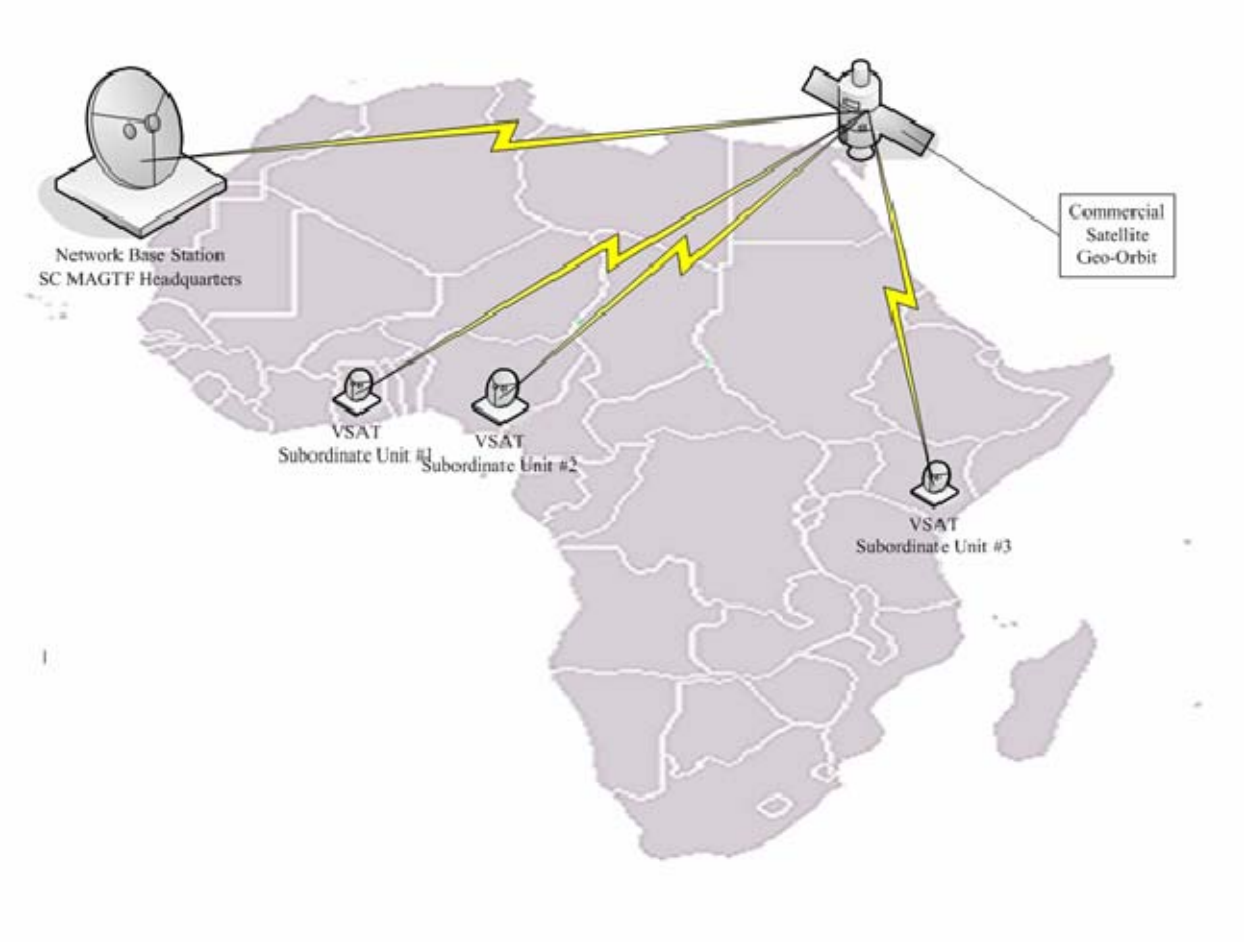

Figure 40. Sample Network Architecture for Security Cooperation MAGTF.

Within this operational concept, and in adherence to the technical and physical description of the Tactical Private Satellite Network that has been illustrated in previous chapters of this work, the headquarters element operating the network base station can

control the parameters of the network, such as bandwidth allocation between terminals. It can also have the ability to remotely manage network devices located at subordinate units. This network entry point would be providing access for each of the subordinate units to the satellite network as well as providing access to information services, such as C2 information (Common Operational Picture, logistics information, and on), electronic mail, web-based services (HTTP, HTTPS), and other types of information services that are required by the subordinate units. Therefore, with the implementation of this network, each of the subordinate units deployed to the various locales around the continent would have reliable network connectivity with the satellite network functioning as the transmission medium. Of course, the headquarters element and the subordinate units all must fall within the footprint of the same geostationary satellite. Should there be an operational scenario in which the headquarters and subordinate units do not fall within the footprint of the same satellite, then some hybrid network must be engineered to provide connectivity. An examination of this concept is outside the scope of this particular work. Access to the satellite link as a backbone can be achieved through the implementation of some wideband networking medium — either cable or through the use of the popular 802.16 WiMAX standard — to extend services even further down the command echelon.

There are several benefits of implementing the Tactical Private Satellite Network within the context of the SC MAGTF. One of the main challenges of having small units dispersed over a large area is that information exchange becomes more difficult. This is because traditional communications, usually found at lower echelons, are relegated to man pack UHF tactical satellite or HF single channel radio — both of which are not able to provide broadband data connectivity. The Tactical Private Satellite Network can provide the required connectivity to address the increased information exchange requirements that would be necessary to facilitate the types of operations illustrated here. The access to biometric data, COP data, and other relevant information on a scale not seen before can enhance the operational effectiveness of company-level organizations. Another benefit of implementing this network is the ability to remotely manage network components. This is especially important because skilled network technicians are

relatively low density and found mostly at the headquarter level. Therefore, the ability to remotely manage the subordinate network devices reduces the impact on personnel structure while still providing reliable network connectivity and performance required.

4. Analysis for Implementation and Application of Tactical Private Satellite Networks in the Coalition Environment

a. Definition of a Coalition

Coalition is defined as "a temporary alliance of distinct parties, persons, or states for joint action" (Merriam Webster's, 237). According to this definition, the important characteristics of a coalition are the following (Zeber et al., 3):

- Temporary: The coalition is formed for a finite time. After that it ceases to exist. The lifetime of the coalition depends on the nature of the action for which it was formed.

- Distinct parties: The coalition members are independent parties who join the coalition voluntarily, but continue to maintain their individual autonomy. One of the parties, however, may act as the coalition leader by the mutual consent of the coalition members.

- Joint action: The coalition is formed for a distinct purpose that presumably could not be achieved by individual action or is achieved more effectively by joint action. Autonomous members acting in concert to achieve a common objective implies that there is a need to share information to support the joint action. The nature of the information sharing will depend on the coalition and its purpose.

The above characteristics can be mapped to the fundamental concepts of the Tactical Private Satellite Network. The tactical aspect goes well with the temporary nature of the coalition because the overall cooperation lasts only for a limited time and it is mission specific. On the other hand, the distinct parties that come together form a private network and the joint characteristic is the fundamental concept of network. They form a network to achieve their common goal and they are the only ones who participate in it.

A coalition need not be political or military. It could exist in any environment, such as a civil or commercial environment, as long as the above characteristics apply. But what really differentiates the coalitions that are intended for utilization is the dynamic nature of the Tactical Private Satellite Network. Such a coalition, whose membership changes over the lifetime of the coalition, is considered a dynamic coalition. A coalition may also be considered dynamic by including mobile infrastructure elements that reconfigure from time to time to meet new requirements. In general, a dynamic coalition is assumed to include both a dynamic membership and a dynamic configuration. Further classification for the sake of this research will be made to differentiate two kinds of dynamic coalitions with respect to their roles and participants: the strict military coalition and the one formed under the pressure of an emergency situation during peace time.

A strict military coalition is a temporary alliance of nations. They contribute military forces to support a joint military operation. A typical multinational military coalition scenario involves the deployment of a multinational Combined Joint Task Force (CJTF) comprising the land, sea, and air forces of the coalition member nations in a hostile region. Their mission is strictly military and involves only military personnel, or other relevantly classified and recruited, to achieve their mission. Their main difference from the above military examples is the plethora of different nations and branches that participate and sensors that can be utilized. Figure 41 depicts such a dynamic military coalition.

The other type of dynamic coalition, to be examined in more detail, is the one formed when first responders to disasters usually need rapid deployment of military, police, fire, and medical units to disaster sites and the establishment of local command posts. Non-government organizations can also participate for the benefit of the whole mission. Coordination is required among all of the deployed first responder units and the command posts, as well as with other civilian groups, such as industrial building owners, and government organizations, such as municipal utilities. Those different participants with their sensors, and their relationships among each other, form an ERN which must be implemented fast and managed accurately to maximize the results of the efforts of its participants — human lives.

If the lack of any friendly terrestrial infrastructure is added to the above characteristics of the two different situations, then the satellite communication channels seem the most — if not the only — reliable solution for the successive implementation of the ERN.

Figure 41. Dynamic Coalition Operational Scenario (from Zeber et al., 6).

b. Analysis for Implementation of the Tactical Private Satellite Network in an ERN

ERNs are formed in specific areas which suffered a major disaster to ensure public safety by addressing different emergencies. When a disaster or crisis situation occurs, communications are frequently incapacitated, non-existent, or completely destroyed. The disaster could cover a small geographic regions or a large one. Depending on the volume of the disaster, usually multiple countries offer their help to cover the area to maximize the outcome of the suffered country's efforts. Generally, the first order of business after a disaster is to send relief workers into the affected region and to establish communications links for them to communicate with the central relief agency and between themselves. By keeping in mind the most probable degradation and destruction — or absence — of terrestrial infrastructure, satellites services, with their

wide geographic coverage (including oceans and seas), are reliable and offer quick deployment. They appear as ideal solutions for relief operations. The outcome, however, of all these different countries' and agencies' efforts that participate in that joint operation under the same footprint of a satellite create a great challenge for the network manager of that newborn ERN.

Instead of creating an imaginary scenario, the ERN that was formed after the major tsunami disaster on December 2004, due an Indian Ocean earthquake with an epicenter off the West coast of Sumatra in Indonesia, will be used. This earthquake triggered a series of devastating tsunamis along the coasts of most landmasses bordering the Indian Ocean. More than 225,000 people in eleven countries were killed and it inundated coastal communities with waves up to 100 feet high (Wikipedia.) The need for humanitarian help was urgent, not only to provide medical care to the thousands of wounded persons, but also to the governmental services, such as public hygiene and transportation, to recover and reassume their duties to relieve the damaged areas. As mentioned above, the first to arrive in the area with the medical personnel were the relief workers to establish communication lines and to connect the different rescue teams among each other and with the rest of the world.

Intelsat was one of the companies that arrived in the area and constructed a Tactical Satellite Network with successful results: it managed to quickly provide complete communication lines to the relief teams (Somji). Following his presentation, as a regional marketing manager of Asia Pacific Intelsat to UNESCAP, it can be seen that they engineered the whole situation. They divided the whole operation into three phases and evolved their Tactical Satellite Network accordingly.

At the first stage the first wave of relief personnel arrived on site and operated in total uncertainties. For that reason, they were best served by personal mobile satellite (Thuraya, Inmarsat, etc.) while the company's personnel were developing the tactical Satellite Network.

Consequently, at the second stage, two to three weeks after the disaster, when small camps started to develop requiring 'thin-route' data/voice connectivity

64/128kbps with <1.8mtr antennas, the newborn Tactical Satellite Network was ready to accommodate their needs. Figure 42 depicts the initial shape of the network which was characterized as the transport phase:

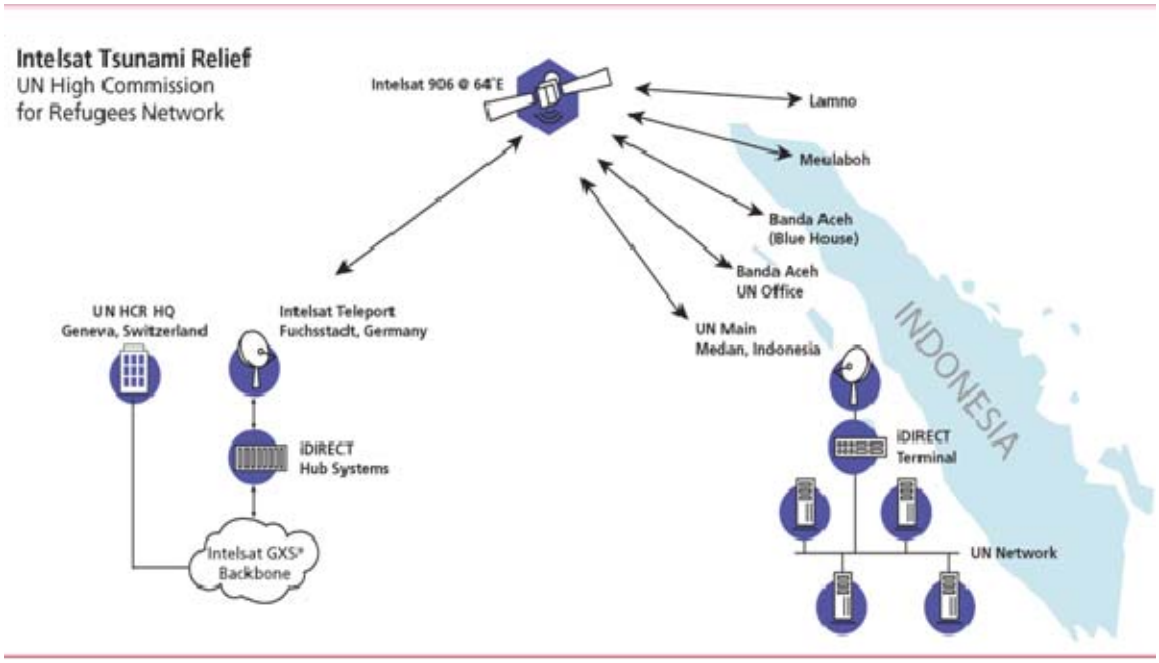

Figure 42. UNHCR Tsunami Relief Network – Transport (From Intelsat Presentation to UNESCAP).

As in any dynamically-formed network, that was not the final form. By continuously evolving the network, they moved to the third stage six to twelve weeks after disaster when larger, permanent relief camps and offices developed. At this stage, agencies, such as UNDP, UNICEF, etc. with larger staff, required bandwidth to satisfy applications (PeopleSoft, Telemedicine, Video Conf, and on) between 512k and 2048kbps. For that reason, the network expanded in order to accommodate the growing needs of the participating agencies. Figure 43 depicts the complete application of the network:

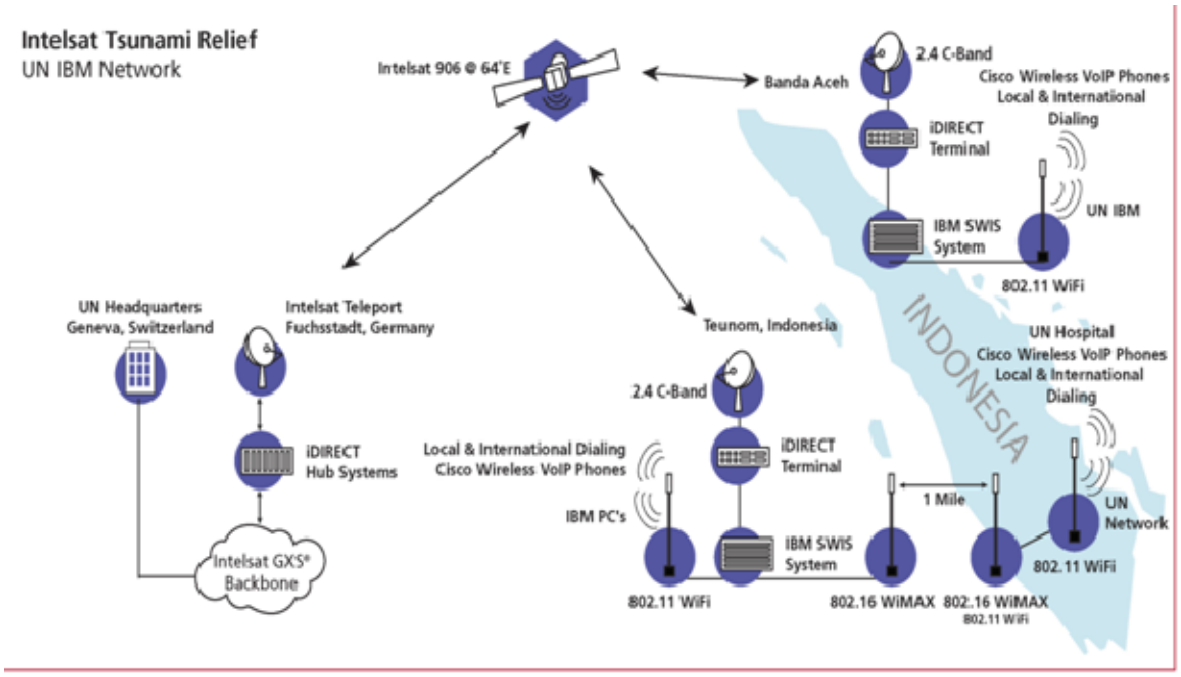

Figure 43. UN IBM Tsunami Relief Network – Application.

The Overall management of the Satellite Network was conducted by the teleport in Germany. According to the company, the teleport acted as CGW and covered the specific satellite with no notable problems. Though a non-mobile base station and far away from the area of interest, this teleport was able to manage this ad hoc and dynamic network because of the large footprint of the satellite. It brought communication services into an area where the terrestrial infrastructure had almost completely been damaged.

Looking outside the box of the specific company, most of the benefits of using such a Tactical Satellite Network for the developing of ERNs can be identified. The following are worth repeating:

- Cost efficiency because of the company's shared hubs and the scaleable space segment because the Service Providers (SP) bought the capacity they needed.
- Flexibility to deploy multiple scalable networks leveraging company's hubs and teleport facilities in C- and Ku-Bands.

- Rapid deployment because of the pre-configured hubs and rapidly deployable equipment.
- Quality of Service and Reliability as defined by the SP and guaranteed by the company because of its global experience; the operated Hubs and Teleports with built-in redundancies and the complete 24/7 management & monitoring of the platform with Level 2, 3 Helpdesk support.

The major difference that the above scenario demonstrates is, compared to previous ones, that the network management was executed by the provider of the satellite bandwidth. In a Tactical Private Satellite Network, however, the management will be executed by a coalitions' designated network manager. As mentioned, the main reason behind a Private network is that keeping the network management "in house" allows better monitoring with more details and focus on the critical aspects specific to the operation. Although a major provider has the ability to conduct network management, this is not its only priority when its services are being shared among different companies with different interests. Network management can be the major task of a mobile base station, deployed by the coalition forces, which can be deployed in the same satellite coverage area with the coalition forces and oversees the proper operation of the different participants. Of course, managing such an ad hoc and dynamic network is challenging, but the end products of self managing specific aspects would compensate for the overhead of management.

In summary, the central problem for any coalition — especially the dynamic ones — is sharing information and infrastructure services efficiently and securely. Control over a member's infrastructure and information must be maintained by the member. Also, the information needed to support the coalition operation must be provided to other coalition members in a timely and secure manner (Zeber et al., 5). Coalition operations require the flexibility to rapidly and securely reconfigure networks and user nodes in real-time and according to its specific needs. Adopting the concept of a Tactical Private Satellite Network and deploying a base station which can conduct the above ad hoc management functions, network management can be more effective and

solve faster and more adequate connectivity problems that coalition's forces may experience in such an "adverse" communications environment.

Overall, it may be said that all the above scenarios demonstrated many common characteristics. For this reason, many of the benefits that a Tactical Private Satellite Network can bring are also applicable to all of them. Above all, ability to manage their own network through advanced control stations and remotely managed network components can guarantee reliable network connectivity and performance required for the conduct of the operations. These commonalities are also the fundamental reasons that the above scenarios can be considered as different flavors of the newly-born nature of operations; Network Centric Warfare.

B. PRIVATE TACTICAL SATELLITE NETWORK AS AN ENABLER TO NET CENTRIC WARFARE

> Net Centric Warfare is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-organization and other network centric operations to achieve commanders' intent (Alberts et al., Network Centric Warfare, 88).

The above statement is used more frequently today as the Information Age where the concept of Net Centric Warfare (NCW), or Net Centric Operations (NCO), has arrived. When NCO are applied to operations other than war, it is ubiquitous and provides a new conceptual framework with which to examine military missions, operations, and organizations. It is used in everyday life, either in DoD or in business operations, and is based on IT-enabled connection among different entities — static or on–the- move — in different places. It enables the collaboration among the participants and optimizes the results of the processes. All the examples in this chapter — military or civilian — are nothing more than net centric operations where the net, or the web, is made by the different participating entities (nodes) through the connecting communications lines (links). It is that connectivity which constitutes the physical domain of NCO — one of its fundamental characteristic: "All elements of the force are robustly networked achieving secure and seamless connectivity and interoperability"

(Alberts et al., Understanding Information Age Warfare, 57). Having assured networking in the physical domain, NCW can move to its informational and cognitive domains and unfold its virtues.

Forming knowledgeable geographically-dispersed forces requires effective linking among the different entities. And this "effective linking" is the ultimate goal of the Tactical Private Satellite Network. By managing the network according to its specific needs, a robust, high-performance information infrastructure can be established that provides all elements of the warfighting enterprise — or the disaster response — with access to high quality information. The whole NCW concept is built around the concept of sharing information and assets which can be enabled only by efficient networking which links battlespace entities together to increase warfighting effectiveness. This allows commanders to get more use out of their entities (Alberts et al., Network Centric Warfare, 94). Consequently, it is the degree to which force entities are networked that determines the quality of information that is available to various forces and their ability to interact in the information domain. For that reason, the quality of networking is the basis of NCW's infostructure and one of the tenets of NCW. It provides the basis of value chain stretching from a set of specific force capabilities to operational effectiveness and abilities (Alberts and Hayes, Power to the Edge, 100-1).

The conceptual framework that employs these tenets is depicted in Figure 44. From the figure, it is derived that this quality of network determines crucial attributes of NCW and further enables operational characteristics, such as the degree of shared information or the quality of Interactions. Thus, without the proper quality of networking, the whole concept of NCW jeopardizes its existence and takes the mission back to the age of Industrial Revolution, when dispersed units remained dispersed and the commanders had to centralize the power, and their units, to drive successful mission. Without NCW, no decentralization can be achieved and no COP can be acquired among the different dispersed participants.

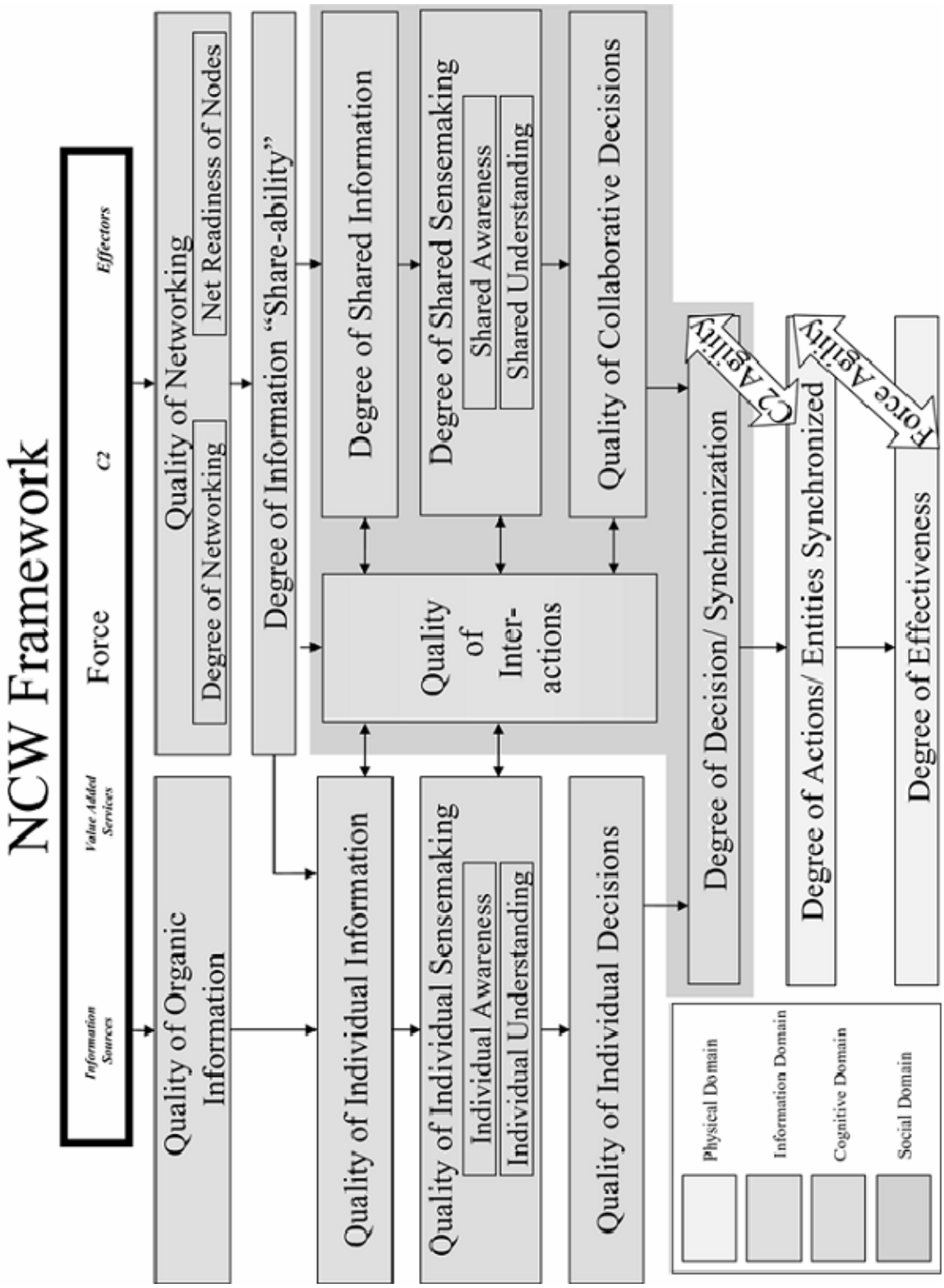

Figure 44. Network Centric Warfare Conceptual Framework (From Alberts and Hayes, 100).

The whole conceptual framework for the Tactical Private Satellite Network is to enable NCW and NCO without having to rely on terrestrial infrastructure or intermediaries who manage the network without having specific interests in it. It envisions giving the power to the operating forces and the power to the edge to manage and optimize the network's connectivity for the best mission. Its global coverage that can be achieved via the satellite needs no existing terrestrial infrastructure and its private nature (managed by the people who participate) aims to create robust communication lines among OTM-dispersed geographical units, between each other, and with their headquarters. This creates effective flow of the critical information that tactical networks handle. The empowered base stations could be the aggregated manager that orchestrates, through effective network management, the effective dissemination of multimedia information among the warfighters in a combat or a peace keeping scenario where coalition forces impose UN regulations or relief forces respond to in an emergency and disaster response situation. After all, "the source of the increased power in a net centric operation is derived in part from the increased content, quality, and timeliness of information flowing between the nodes in the network" (Alberts et al., Network Centric Warfare, 100).

THIS PAGE INTENTIONALLY LEFT BLANK

V. TACTICAL PRIVATE SATELLITE NETWORK REMOTE NETWORK MANAGEMENT EXPERIMENTATION AND CONCEPT DEVELOPMENT

Up to this point, the examination of the Tactical Private Satellite Network has included several aspects. The first area of this study concentrated on the current and future states and trends in the commercial and military satellite communications field. From there, the authors formulated the concept of and submitted a proposed definition for the Tactical Private Satellite Network. Additionally, the study included a treatment of networks that were characteristically similar to the proposed concept that are currently deployed in support of the military domain, various civil government agencies, and within the private sector. The last idea that was examined was the conceptual implementation of the Tactical Private Satellite Network within various operational domains of interest. This chapter will deal with aspects of management of the Tactical Private Satellite Network — specifically, remote network management, relevant experimentation of the illustrated concept, the results of the experimentation, and the formulation and proposal of a management construct to address the issues of managing this specific network.

A. HYPOTHESIS AND PURPOSE OF EXPERIMENTATION

One of the key principles put forth through the development of the concept of this Tactical Private Satellite Network is how the network, consisting of the network devices (routers, switches, wireless access points, and on) which connect end users and the satellite terminals that provide the actual transmission path, is managed as a single entity with the ultimate goal of providing robust services. It is suggested that this network, in its holistic form, can be managed from a single point within the network — specifically with the implementation of the base station/gateway concept that was defined in Chapter III. Thus, the gateway will facilitate the agent function in network management by serving as the advanced agent for actively managing the network. Also, there must be consideration given to the limiting distribution of trained networking personnel and to the possibility that participating members in the network may not have trained networking personnel

assigned to their operational facilities. Therefore, there is a need for a capability to conduct advanced network management from a remote location. The bandwidth provided by the satellite link can be used as a path for this functionality. The hypothesis behind the experiment is that the concept of remote network management can be illustrated: remote management of this holistic network is practical and can be executed within the architecture of the Tactical Private Satellite Network. This testing will also serve as a basis for further research and experimentation within this realm. To this end, an experiment is designed to test the feasibility and functionality of remote network management within the context of the Tactical Private Satellite Network.

B. TESTING/EXPERIMENTATION SCENARIO

The scenario used for this test and experimentation closely aligns with the operational implementation illustrated in Chapter IV section A3 of this thesis. Specifically, the scenario of interest is the SC MAGTF. The purpose of this experiment is to demonstrate the capability of remote network management at MCTSSA with regard to a portion of the bandwidth that can be used to perform management functionality or the entire satellite link that can be utilized as a network management control channel. For details on the operational aspect of the implementation, the reader may refer to the relevant section in Chapter IV. Theoretically, deployed units that have implemented the Tactical Private Satellite Network are able to effectively exchange information between higher headquarters and subordinate units and laterally between subordinate units. Essentially, communication is bi-directional in nature. An important aspect of the research associated with this operational concept and the conceptual framework for a Tactical Private Satellite Network is the ability to conduct network management remotely. Several assumptions have been generated to guide the experimental design. The suggested assumptions are as follows:

- Security Cooperation MAGTF Company deployed beyond doctrinal distances and BLOS Radio Frequency capabilities. These units are forced to utilize BLOS or OTH technology for communications with higher, adjacent, and supporting units.
- SATCOM coverage available in Area of Responsibility (AOR) (commercial or MILSATCOM).

- Swe-Dish IPT (satellite terminal device) technology fielded at Battalion (Bn)/Company (Co) Headquarters (HQ) as SATCOM link.

To effectively test the concept of the Tactical Private Satellite Network within the context of the SC MAGTF, it is important to outline the information exchange requirements related to this operational implementation. There are sixteen specific events that involve an exchange of information from subordinate headquarters to higher headquarters. These events should be considered the minimum amount of traffic that will be passed over the SATCOM link. For the purposes of this experiment, all events are simulated and represent multiple different application protocols, such as chat messages, e-mail attachments, and e-mail main body.

1. Experimental Architecture

The architecture for the experiment is a representative network, similar to what would be deployed in to support the SC MAGTF. The operational concept was illustrated in Chapter IV. This test network is made up of two nodes: one represents a higher headquarters and one represents a subordinate headquarters. The latter is designed with the intent to replicate the packet-switched network that would be deployed to facilitate information exchange requirement in both directions — from higher headquarters to the subordinate headquarters and from subordinate headquarters to higher headquarters. The test network is a routable network that relies on a satellite link for connectivity. The nodes were connected via satellite point-to-point link using the Swe-Dish IPT suitcase terminals that are the property of the NPS CENETIX lab. The Swe-Dish IPTs are a representative transmission system because they are not currently fielded to operational units within the Marine Corps. For the purpose of the experiment, the Swe-Dish suitcases have similar capability as fielded systems. The satellite that was accessed during the experiment was the Telstar 7 (Galaxy 27) satellite that is in geostationary orbit with position location of 129 degrees west (http://www.n2yo.com/satellites/?c=10). Figure 45 illustrates the position of the Telstar 7 satellite relative to the testing site. Satellite access and bandwidth, as well as testing facilities, were provided courtesy of the MCTSSA located in Camp Pendleton, California.

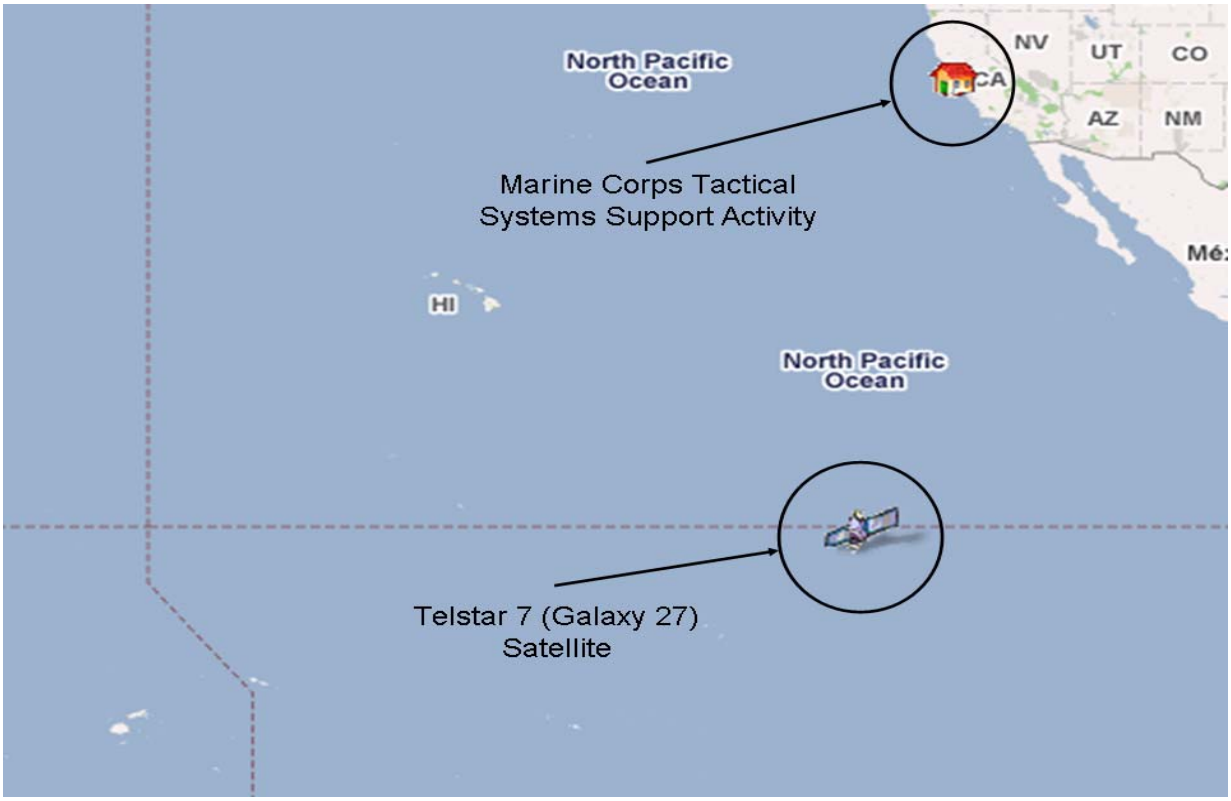

Figure 45. Telstar 7 Satellite Location (from http://www.n2yo.com/?s=25922).

The remainder of the test network topology consists of hosts, switches, and routers — all networking devices that would be found supporting deployed units. Figure 46 details the network architecture utilized for the experiment. The satellite point-to-point link was engineered to initiate a router-to-router connection between the notional operating units. Since the routers have a direct connection through the satellite link to each other, this test/experimentation network closely replicates the proposed conceptual architecture of the Tactical Private Satellite Network. The hosts on the network were running Windows XP operating system. One host at the higher headquarters node functioned as the network management agent. This management agent was running the commercial software SolarWinds Engineering Edition as the network management application and was responsible for collecting data on network performance and was the originator of network management-related tasks:

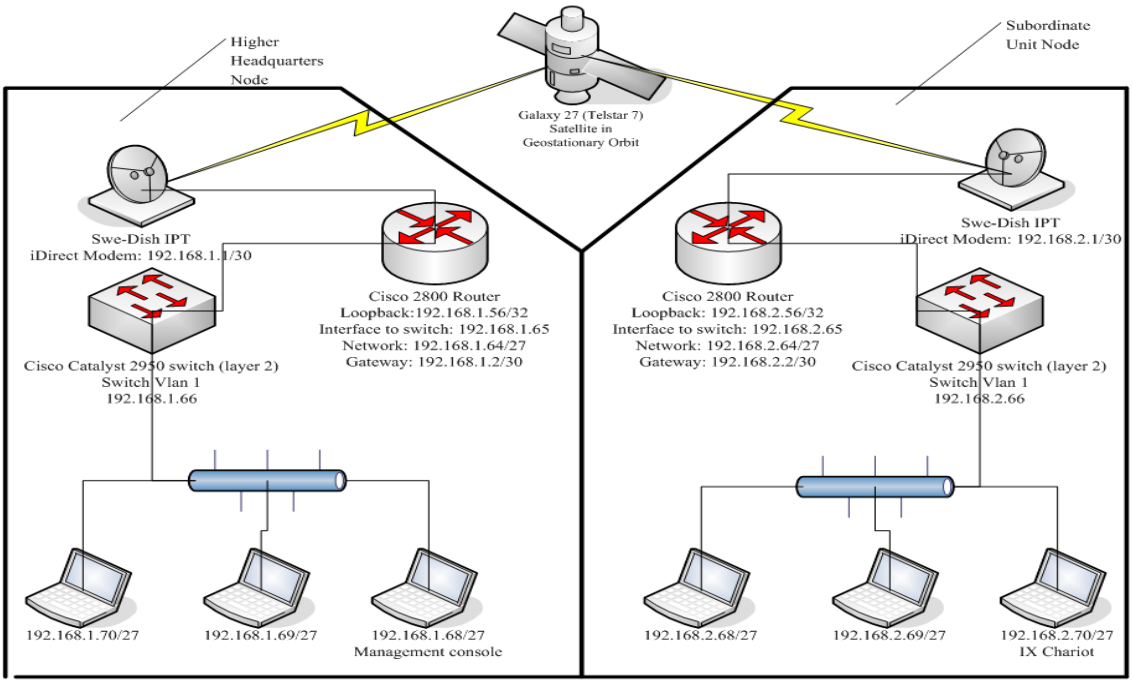

Figure 46. Experimental Network Architecture.

In addition to running SolarWinds, the management host was also running the traffic analyzer WireShark. It was used to capture packets traversing from the management agent to the rest of the network. The management agent for the satellite transmission portion of the network was also located at the higher headquarters node. It was running the iSite software, a proprietary software package specifically used for the monitoring of the iDirect modems that are embedded in the Swe-Dish IPTs. Information exchange requirements between the nodes were determined prior to the experiment and, since those requirements were determined, data needed to be created to represent the flow on the network. To create data to flow over the network, the IX Chariot software was employed and resident on a host at the subordinate unit node. The purpose of the IX Chariot was to create and transmit messages using specific protocols to replicate operational traffic traversing the network. This data replication would serve to give some estimation as to the utilization of the satellite bandwidth while exchanging certain types of data across the satellite link. Specifics on types of data transmitted are detailed in a subsequent section of this chapter.

In addition to the diagram of the test network architecture shown, Table 7 is provided to illustrate the detailed router and switch configuration highlights and relevant IP addressing for the test network:

Device/Interface	IP Address	Notes
Battalion Node		
Swe-Dish iDirect Modem	192.168.1.1/30	
BN_ROUTER		Cisco 2800 series
Loopback	192.168.1.56/32	
Gateway	192.168.1.2/30	Fast Ethernet Port 0/0 – connection from router to Satellite modem
Network	192.168.1.64/27	
Interface	192.168.1.65	Fast Ethernet Port 0/1 – connection from router to switch
BN_SWITCH		Cisco Catalyst 2950 Switch (24 port)
Vlan	192.168.1.66	
Company Node		
Swe-Dish iDirect Modem	192.168.2.1/30	
CO_ROUTER		Cisco 2800 series
Loopback	192.168.2.56/32	
Gateway	192.168.2.2/30	Fast Ethernet Port 0/0 – connection from router to Satellite modem
Network	192.168.2.64/27	
Interface	192.168.2.65	Fast Ethernet Port 0/1 – connection from router to switch
BN_SWITCH		Cisco Catalyst 2950 Switch (24 port)
Vlan	192.168.2.66	

Table 7. Detailed IP addressing Scheme for the Test Network.

Although the test network depicted is representative of the Tactical Private Satellite Network, it is necessary to point out several differences, and the associated ramifications related to those differences, between the network that was used to test and

the conceptual model that was first defined in Chapter III. First, the transmission architecture for the test network is in a point-to-point configuration. The concept of the Tactical Private Satellite Network requires, for most operational implementations outlined in Chapter IV, a point-to-multipoint configuration (multicast). This is critical to note in that in the point-to-point configuration, only two nodes share finite satellite bandwidth; whereas, the point-to-multipoint model will dictate that at least two nodes — if not more — will be sharing the bandwidth. This will require that efforts, associated with acquiring commercial satellite bandwidth to support the Tactical Private Satellite Network, are undertaken with the knowledge and understanding that more nodes will require more resources from the satellite. The second difference is that there was no tactical network entry point/satellite base station that was associated with the test network. Again, as outlined in Chapter III, the essence of the Tactical Private Satellite Network is the employment of a base station/gateway that functions as the NECOS for the satellite transmission portion of the network. Therefore, without the employment of the base station during testing, the true management capability could not be evaluated. Due to the proprietary nature of the iDirect modems that are embedded in the Swe-Dish SATCOM terminals, no actual management of the modem could be accomplished. As with the MIO 08-2 experiment illustrated in Chapter IV, because no access to the satellite terminal modem could be acquired, the terminal operators were relegated to the role of monitor. This is a critical point in that to effectively manage the satellite network portion of the Tactical Private Satellite Network, and to view the network as a holistic network consisting of the satellite transmission piece and the networking devices, a base station/gateway NECOS with the capability to actively manage the performance of the satellite terminal modem needs to be employed. Finally, it is important to note that no encryption was utilized on the satellite transmission. Although encryption is required by the Department of Defense Instruction (DoDI) 8100.2, the satellite link for the experiment was commercial-based. Also, since the test network was closed (no other participants), it was decided that there was no urgent need to encrypt the experimental traffic. The Cisco 2800 series routers that were employed on the network were capable of employing Advanced Encryption Standard (AES) encryption. Because of time constraints

associated with the experiment, the AES encryption was not employed. Conjecture is that the employment of encryption on the network will affect the overall throughput of the satellite link; therefore, the actual performance of the link that was monitored and recorded during the test was artificially elevated. There are other elements of security and encryption, such as VPNs, and Public Key Infrastructure (PKI), that are relevant, but they were not tested during this experiment.

2. Metrics of Interest

To test the legitimacy of the network configuration, the applicability of a satellite communications link and the ability to remotely manage network devices from a central location is necessary to collect information relevant to the experiment. The items that were to be investigated drove the selection of the metrics and the data collected. The following questions served as the basis of investigation during the testing/experimentation:

- How does the satellite link perform with regard to information exchange?
- How do networking components (routers and switches) perform through this particular link?
- Does the use of network management protocols (ICMP, SNMP, and TELNET) work over the satellite link?
- How much bandwidth, as a portion of the aggregate, does management-related data consume?
- Does the injection of network management-related traffic over the link adversely affect the flow of operational data?

A determination was made as to what data should be collected and another was made as to what associated metrics would be useful to provide answers to the previously listed questions. Table 8 illustrates the data of interest, the metric, and the rationale behind the collection of that piece of data:

Metric	Collection Method	Rationale
Packet Loss	SolarWinds	To note the performance of networking devices deployed
Satellite Link Throughput	iSite	Illustrates the capability of the established satellite link
Router performance (Minimum/maximum response time and packet loss) per interface	SolarWinds	Used to determine overall performance of the routers on the network
Switch performance (Minimum/maximum response time and packet loss) per interface	SolarWinds	Used to determine overall performance of the switches on the network
Transmission Speeds per node	SolarWinds	To determine the transmission rate per each node in the network
Transmission of ICMP	WireShark	To illustrate the use of ICMP through the network
Transmission of SNMP-related data	WireShark	To illustrate the path of the SNMP messages throughout the network topology

Table 8. Metric, Collection Method and Rationale.

At this point, both the test architecture and the desired data to be collected have been determined. The next section illustrates the execution of the experimentation to include the methodology, the data collected, and the actual results ascertained from the collected data.

C. EXPERIMENT EXECUTION

The experiment was executed from 4 to 7 August 2008 at the Marine Corps Tactical Systems Support Activity in Camp Pendleton, California. MCTSSA furnished access to and use of the facilities in the SWAN lab. The nodes for the experiment were named Battalion, representing the higher headquarters, and Company, representing the subordinate headquarters. This naming convention is consistent with the test scenario illustrated earlier in this chapter. It is also consistent with the SC MAGTF operational implementation outlined earlier in this research. The two Swe-Dish IPT satellite terminals

were installed and configured for use in the point-to-point mode. Concurrent to the installation and activation of the satellite communications link, the network devices were installed and the routers and switches were configured to operate within the parameters of the network. Once the satellite link was established and all of the networking components were installed and tested, the network management agent conducted a discovery to establish the baseline of the network. To be more specific, the management agent conducted a discovery sweep of the network utilizing the Packet Internet Groper (PING) sweep utility included in the SolarWinds tools. Figure 47 is data that was collected as a result of the network discovery using PING Sweep. From the output provided, the PING sweep utility determined that the response time from hosts and network devices that were resident on the Company Node network had a response time of over 500 ms, which is consistent with response time associated with communications through a satellite at GEO:

IP Address	Response Time	DNS Lookup	Notes
192.168.1.0	1 ms		
192.168.1.1	1 ms		Swe-Dish IPT (BN node)
192.168.1.2	0 ms		BN Router Interface FA 0/0
192.168.1.3	0 ms		
192.168.1.56	1 ms		BN Router Loopback
192.168.1.64	Bad Destination Address		BN Router Network
192.168.1.65	1 ms		BN Router Interface FA 0/1
192.168.1.66	1 ms		BN Switch Vlan address
192.168.1.67	Request Timed Out		
192.168.1.68	0 ms	CF74-TB-01	Management agent
192.168.1.69	0 ms	OROS	host
192.168.1.70	0 ms	CF74-TB-03	host
192.168.1.95	0 ms		
192.168.1.255	1 ms		
192.168.2.0	Request Timed Out		
192.168.2.1	505 ms		Swe-Dish IPT (CO node)
192.168.2.2	508 ms		CO Router Interface FA 0/0
192.168.2.56	505 ms		CO Router Loopback
192.168.2.64	505 ms		CO Router Network
192.168.2.65	506 ms		CO Router Interface FA 0/1
192.168.2.66	503 ms		CO Switch Vlan address
192.168.2.67	Request Timed Out		
192.168.2.68	505 ms	ORGANIZT-ED6C68	host
192.168.2.69	504 ms	ORGANIZT-14AA7D	host
192.168.2.70	504 ms	DELLD820	IX Chariot
192.168.2.95	504 ms		

Figure 47. PING Sweep Utility Results.

In addition to the discovery of the packet switched network, a baseline of the actual performance of the satellite link was also obtained. Again, using the proprietary iSite software package, a baseline was taken of the satellite link used during the

experimentation. Figure 48 illustrates the baseline of the transmission path associated with this test. The ICMP and UDP traffic that is seen on the baseline is the result of the PING Sweep that was executed concurrently to the capture of the transmission baseline. Once the baseline configuration of the network was captured, the actual testing and experimentation had begun:

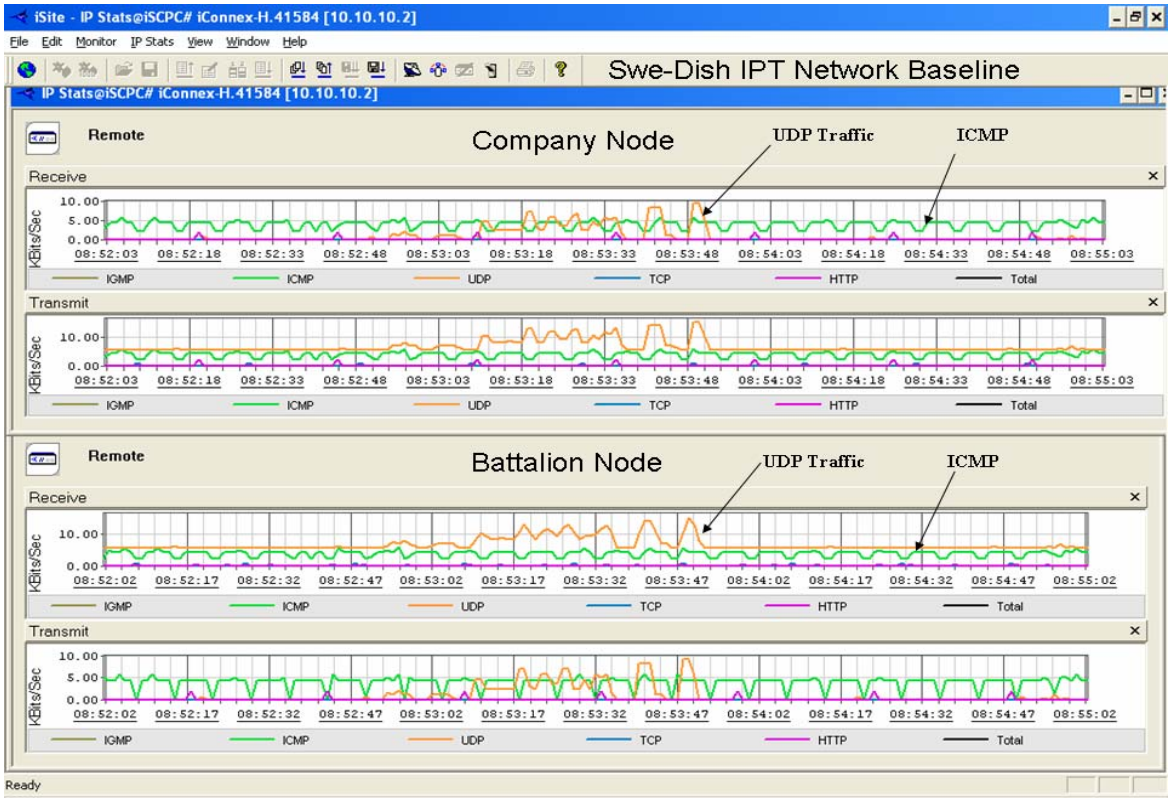

Figure 48. Baseline of Satellite Link.

1. Methodology

Simulated data relevant to the scenario outlined previously in this chapter was generated using the IX Chariot software application and transmitted across the satellite link from the Company Node to the Battalion Node. Network performance data was collected using commercially available network management software tools. The management agent was utilizing standard protocols to conduct management of the network. These protocols include the SNMP, the ICMP, and TELNET. These tools are

available to any network manager either through the command prompt terminal window or as they are employed within software applications, such as SolarWinds. In addition, a protocol analyzer was employed to capture packets traversing the network to allow for the analysis of data. Once the management agent was configured and the baseline of the network, both the devices and the satellite communications link were captured and the simulated data packages were transmitted.

2. Test Plan Narrative

There were three equally important goals with regard to the testing. The first was the overall performance of the satellite link; the second was the ability to capture and analyze network performance; and the third was the ability to remotely manage network devices. Therefore, to get test results that would verify the potential of the satellite link within the context of the test scenario, and to track and manage the performance of the networking devices that were deployed, a total of nineteen test runs were conducted. Each test run consisted of commonly used applications (Layer 5 of the Open Systems Interconnection (OSI) reference model) protocols, such as Simple Mail Transfer Protocol (SMTP) version 1, the File Transfer Protocol (FTP), and on to gauge network performance. As the testing progressed, multiple application protocols were run concurrently to stress the network and to determine the operating capability. In addition to the transfer of application protocols across the network, the management agent set a polling interval for SNMP data at 120 to 240 seconds. This frequent polling rate introduced an increased amount of data across the network. It aided to further understand network performance and accounts for the constant presence of ICMP and UDP data on the performance results. The amount of management data that was injected into the network was done to replicate active management of multiple stations or subnets across the network. For the sake of this study, five of the nineteen test runs were chosen to exhibit the performance of the network — both the satellite link and the networking devices. Those five simulated data samples represented information exchange requirements called for by the testing scenario illustrated previously. The five representative tests were:

- Internet scripts: SMTP to simulate the use of e-mail.
- Internet scripts: FTP to simulate a file transfer from a server residing at the battalion node requested by a host on the company node.
- Internet Relay Chat (IRC): a commonly used chat application.
- Collaboration utilizing Microsoft NetMeeting (video and text chat) and the TELNET protocol: simulating a diverse amount of traffic concurrently traversing the network.
- Collaboration utilizing Microsoft NetMeeting (video and text chat), file transfer, and desktop share: simulating concurrent diverse application utilization.

3. Results

Since there is no means to manage the network in its holistic form, the performance of the network is broken down into three sections. That is to say that separate management agents were required and used for the satellite link and for the other network devices. The first section will illustrate the performance of the Swe-Dish IPT satellite terminals during the experimentation as captured by the proprietary iSite software. The second section will illustrate the overall performance of the networking devices (the routers and switches) through the duration of the testing as captured by SolarWinds. The final section will illustrate that management related data, such as ICMP and SNMP traffic, was successfully sent over the network and was recorded by the traffic analyzer, WireShark. Once the performance results have been illustrated and explained, general conclusions will be drawn and delivered.

a. Performance of Swe-Dish Satellite Terminals

For the experiment, we were allocated a 1Mbps uplink and 1Mbps downlink. The performance of the Swe-Dish IPT satellite link was consistent in that no outages were recorded for the duration of the experiment. There were some issues associated with establishing the initial connection, but, after the connection was finally established, the satellite link remained solid. As expected, the performance of the satellite terminals seemed consistent with that which was noted during the MIO 08-2 experimentation.

The first test that was performed was the simulated transfer of SMTP related data. This test was to simulate the use of electronic mail from the company node to the battalion node. This simulation was chosen because e-mail has become ubiquitous with regard to information dissemination and collaboration within the military. The data transfer was recorded and is illustrated in Figure 49. The preponderance of the traffic noted (the saw-tooth pattern) is the TCP connection and transfer between nodes.

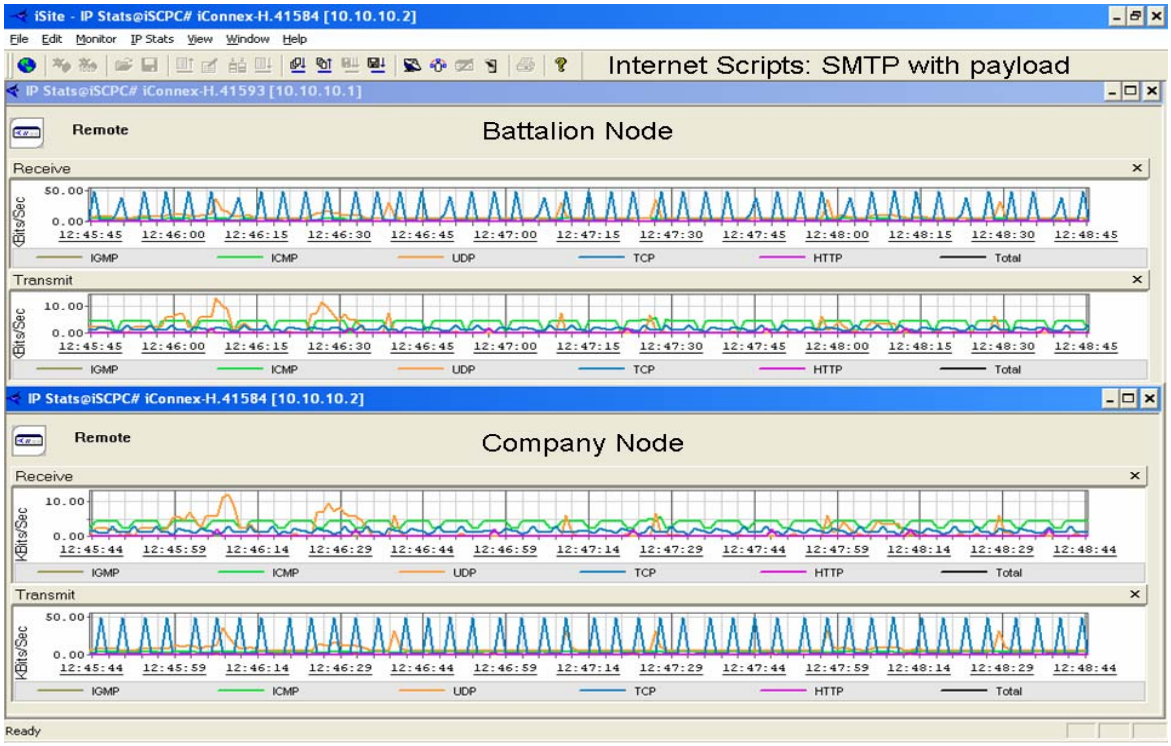

Figure 49. Simulated SMTP.

The second test sample consists of the performance during an FTP active mode session. Active mode FTP transfers data in a different way than passive FTP and also in a way that is counter-intuitive with regard to the TCP standard. This is because it does select port 20 as its source port (not a random high port that's greater than 1024) and connects back to the client on a random high port that has been pre-negotiated on the port 21 control connection (http://www.crossftp.com/kb/entry/20/). Therefore, the client is initiating the control session as well as the data transfer session. In this example, the

company node is transferring a notional file from the battalion node. Figure 50 illustrates the FTP session. Like the SMTP sample, TCP traffic makes up the preponderance of the load on the link during this test:

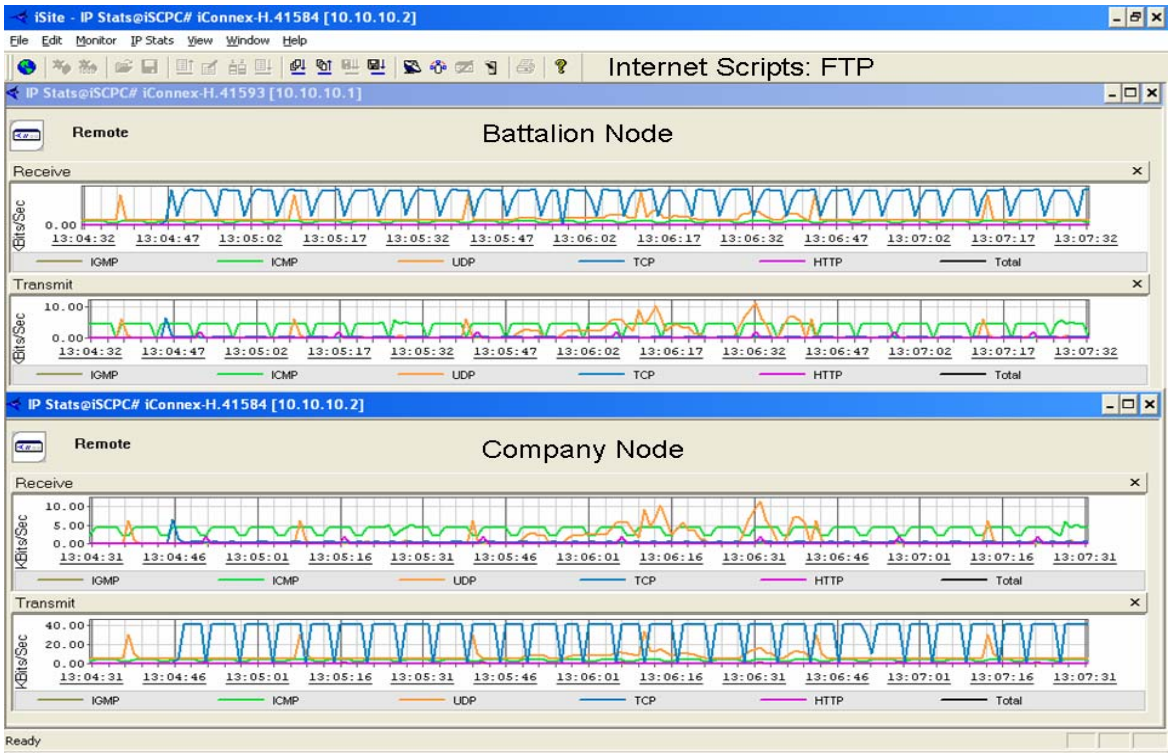

Figure 50. Simulated FTP session.

The third test of interest is a simulation of the popular collaborative tool, the IRC. Figure 51 illustrates the link performance during a simulated IRC session between nodes. An IRC session uses the TCP standard to make connections between clients and servers. Once the TCP connection is made, a UDP datagram containing the line of text chat is sent. As the graph shows, there is an increase in TCP traffic on both the send and receive sides of each node.

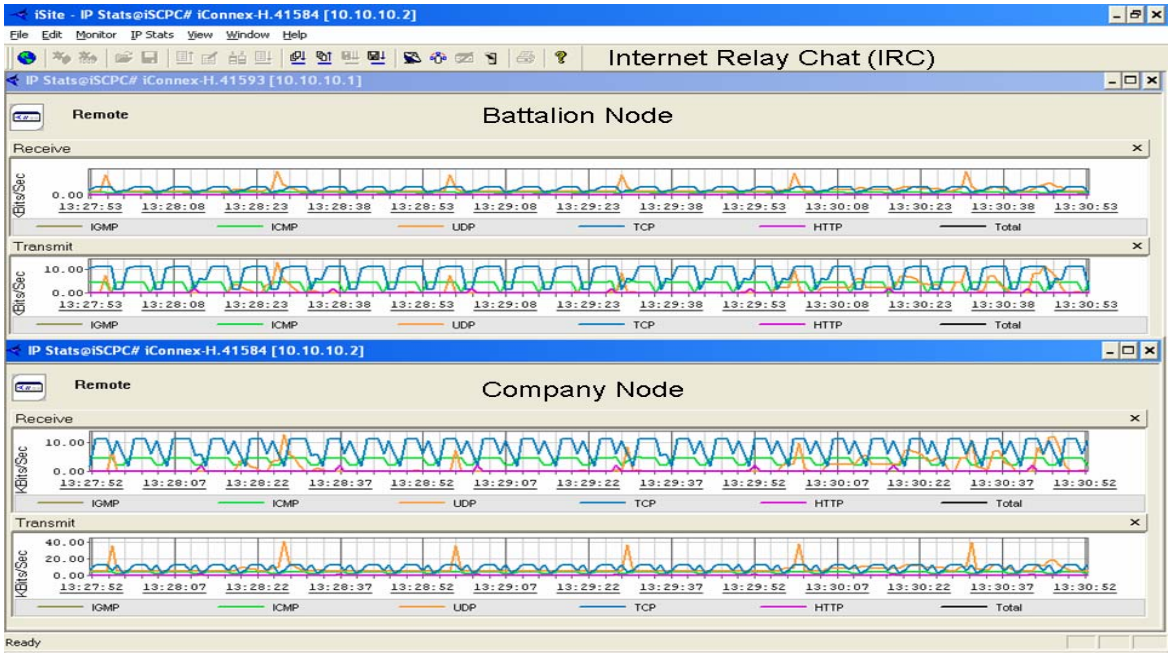

Figure 51. Simulated IRC Session.

So far the simulations have demonstrated one application protocol traversing the network at a time. The exception to this is the constant UDP and ICMP traffic automatically generated by the network management agent and purposely injected onto the network. The subsequent two tests illustrate the performance of the satellite link while multiple application protocols are being transmitted simultaneously. This is concurrent with the constant level of management-related data. A TELNET session was added to the subsequent tests and initiated at the management console (located on the battalion node) to the router located on the company node. Thus, the TELNET session had to traverse the satellite link — just as the other traffic — and the effects were captured within the context of link performance.

The fourth test that is illustrated is a simulated collaborative session utilizing the Microsoft NetMeeting application. During this session, both video and text chat were used. Additionally, a TELNET session from the battalion node to the router on the company node was executed.

Figure 52 illustrates the performance of the link during this simulated data exchange. The majority of the data in this case is UDP. This is because of the connection-less nature of the streaming video. Previous simulations have been more oriented towards TCP:

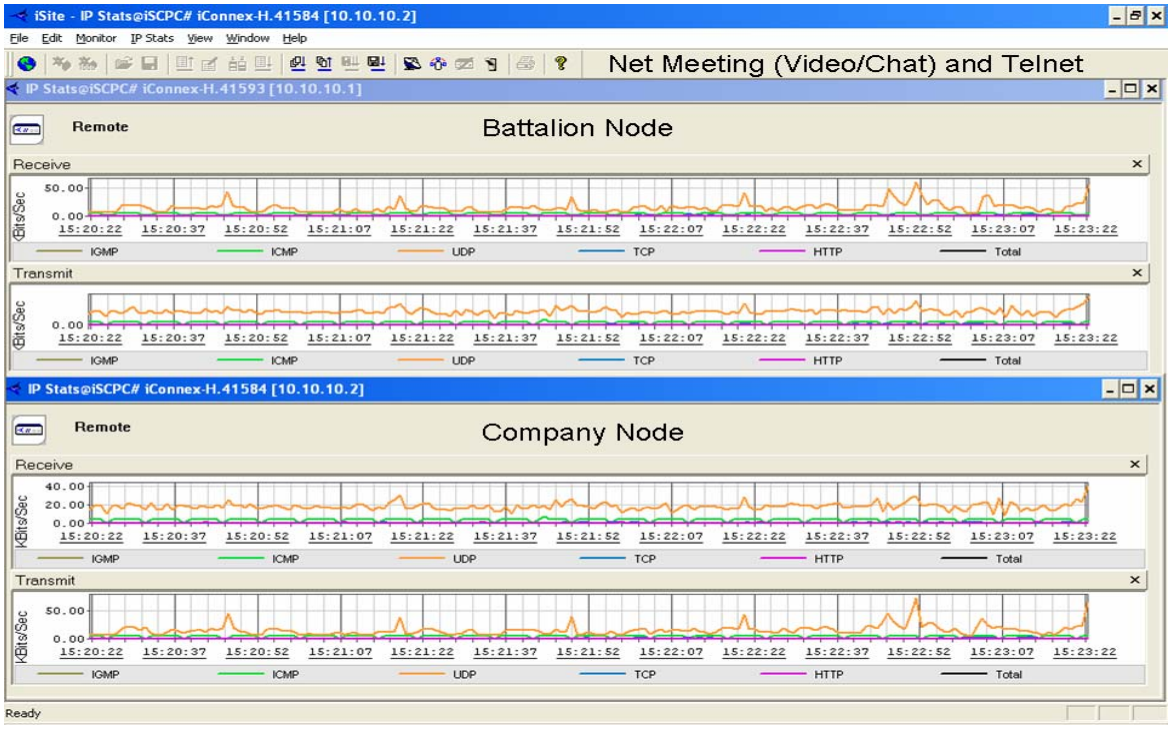

Figure 52. Simulated Multi-Application Exchange with TELNET Session.

The final simulation was the most comprehensive, and was originally developed to stress the satellite link. This particular simulation, the last of the sample five, consists of multiple application protocols being transferred simultaneously — specifically a NetMeeting (video and text chat) session, a file transfer, and a desktop share. Figure 53 illustrates this particular test. As demonstrated in the graph, there are increased amounts across the application protocols (UDP, TCP, and HTTP). According to the Microsoft TechNet website, NetMeeting utilizes the TCP standard for data transport and call control and uses the UDP standard for secondary connections for sending and receiving audio and video (http://technet.microsoft.com/en-us/library/cc767134.aspx).

The information available on the web resource is consistent with what was illustrated in the test results. As with the previous four samples, the presence of the ICMP and SNMP management data is purposely injected by the network management agent. In comparing this last sample with the previous, there is a marked increase in the receive/transmit kilobits per second (Kbps) on each of the two nodes. It is, therefore, suggested that this last sample test more closely represents the actual operational information exchange that would be present in a Tactical Private Satellite Network.

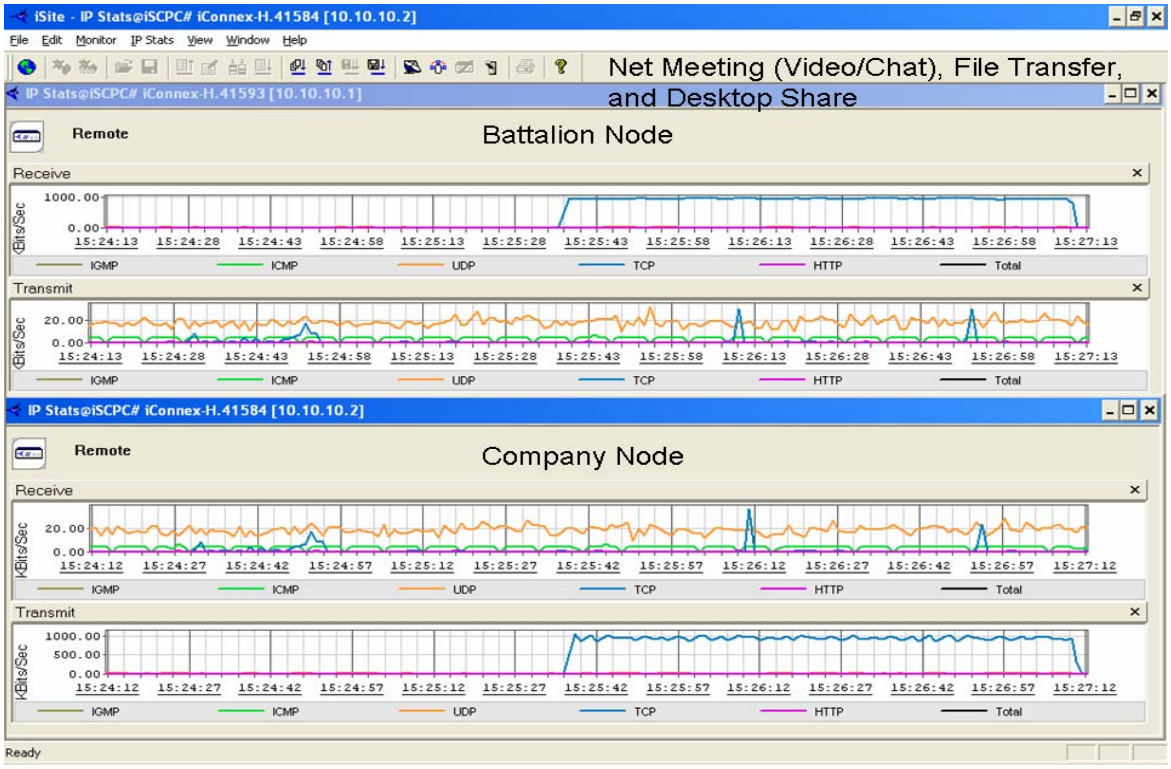

Figure 53. Simulation of Multiple Application Protocols Transmitted Simultaneously.

In summary, the performance of the Swe-Dish IPT terminals connected through a commercial communications satellite in geostationary orbit met all expectations and matched the performance characteristics that were recorded during previous experimentation. Even though the allocated bandwidth from the commercial provider was 1Mbps for each uplink and downlink, at peak traffic only about 500 Kbps

was utilized. The reduction in bandwidth available is a limitation of using satellite terminals with small antennas (in this case, 0.9 meters) and, as such, these terminals are considered disadvantaged terminals. To compensate for the point-to-point topology between two disadvantaged terminals, more resources are required from the space segment to close the link. Thus, even though 1Mbps was leased, the resource requirements to close the link left only half of the bandwidth available for actual data transmission. As demonstrated by the collected data, the satellite link terminated by these particular terminals was capable of handling a wide assortment of simultaneously transmitted application protocols — in addition to network management-related data. As noted previously, the proprietary iSite software provided only the capability to monitor the performance of the iDirect modems. Due to the proprietary nature of the software, there is no management functionality included or authorized by the manufacturer.

b. Performance of Network Components

Not only was the performance of the satellite terminals of interest during this experimentation, but it is also crucial to examine the performance of the networking devices within the context of a satellite-based routable network. Considering that the devices were connected via a transmission path with well-known delay (geostationary satellite delay of roughly 500 ms), and since the Tactical Private Satellite Network will most likely use geostationary satellite as the primary means of connectivity to circumvent the limitations associated with LEO satellites' constellation, such as low available throughput and need for ISL connections, the data gathered from this experiment would be germane to the conceptual network architecture. For the sake of gathering data and conducting analysis, the performance of these devices was compared with each other. For instance, the router at the battalion node was compared with the performance of the router at the company node. Likewise, a comparison was undertaken with regard to the switches that were employed. These side-by-side comparisons are possible because each node had the same hardware with the same configuration as its counterpart on the distant end. This was done to eliminate any variance that might have been introduced by the difference in equipment and configurations. As noted previously, SolarWinds was used to capture relevant data on the performance of the devices in question during the experimentation.

Since, by definition, the network is routable, the first devices to be examined were the routers. The test network used Cisco 2800 series routers — one at each node. Both routers were furnished by MCTSSA for the duration of the experiment and each was configured on-site prior to the execution of the experiment. The purpose of each router was to function as the gateway between the network and the satellite terminal. Each interface on the routers was configured for the same purpose to maintain consistency. In terms of detailed configuration, the Fast Ethernet port 0/0 was configured as the gateway connection to the modem on the satellite terminal; the Fast Ethernet port 0/1 was configured as the connection between the routers and the respective switches. The data collected was mostly concerned with those particular ports because all data must traverse through them to be either transmitted through the satellite link or routed and delivered to hosts on the subnet. Figures 54 and 55 demonstrate the MIN/MAX response time (in green) and packet loss for each of the routers in total. This provides a detailed picture of the overall router performance. Again, noting the response time of the Company Router as at least 500 ms, it is consistent with the characteristics of a geostationary satellite communications link. The response time for the Battalion router was relatively low because the performance data was captured locally at the Battalion node. With regard to the Fast Ethernet ports (Fa 0/0) on both routers, the performance in terms of the MIN/MAX bps received, MIN/MAX bps transmitted, and Average Receive bps, and the Average Transmit bps showed little variation in a side-by-side analysis. Figure 56 and 57 illustrate the performance characteristics of this interface for each router. This data demonstrates that the performance of this particular interface and the interface between the router and the satellite terminal were able to handle the simulated transmission load. Even though the capacity of the routers is roughly five orders of magnitude more than the satellite link, it was deemed necessary to the concept of remote management to examine these network devices within the context of the experiment.

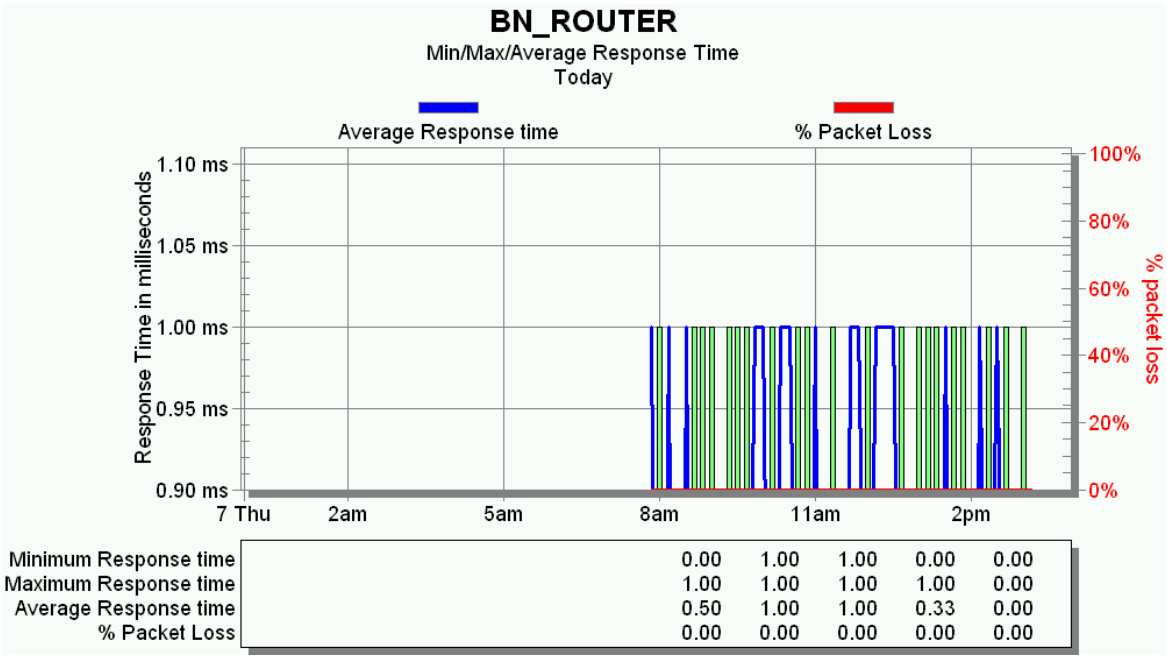

Figure 54. BN Router Performance Summary.

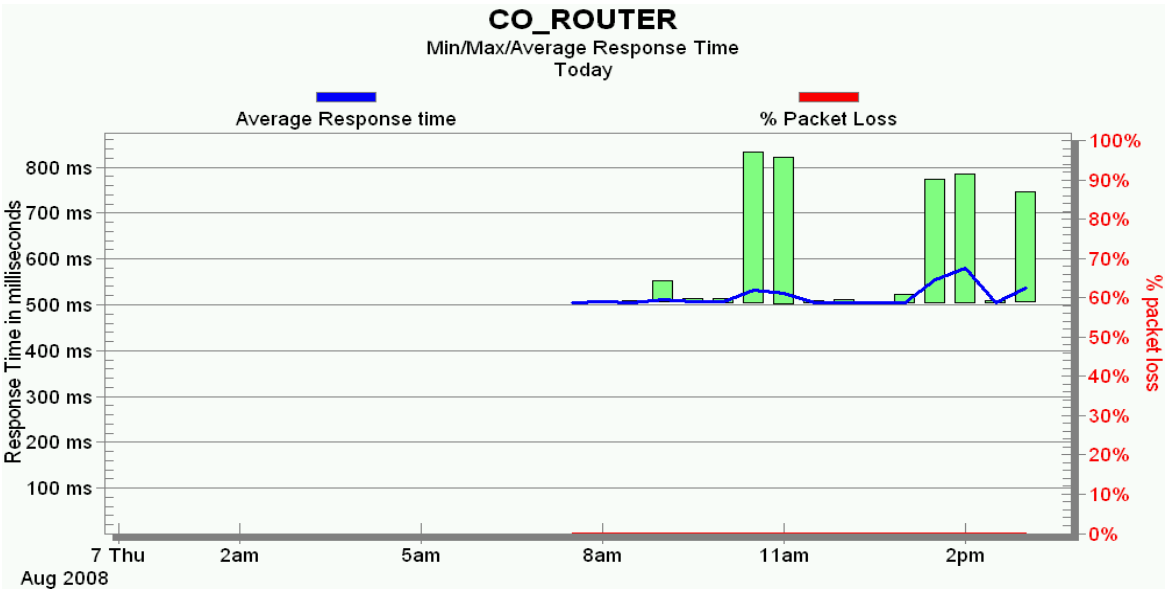

Figure 55. CO Router Performance Summary.

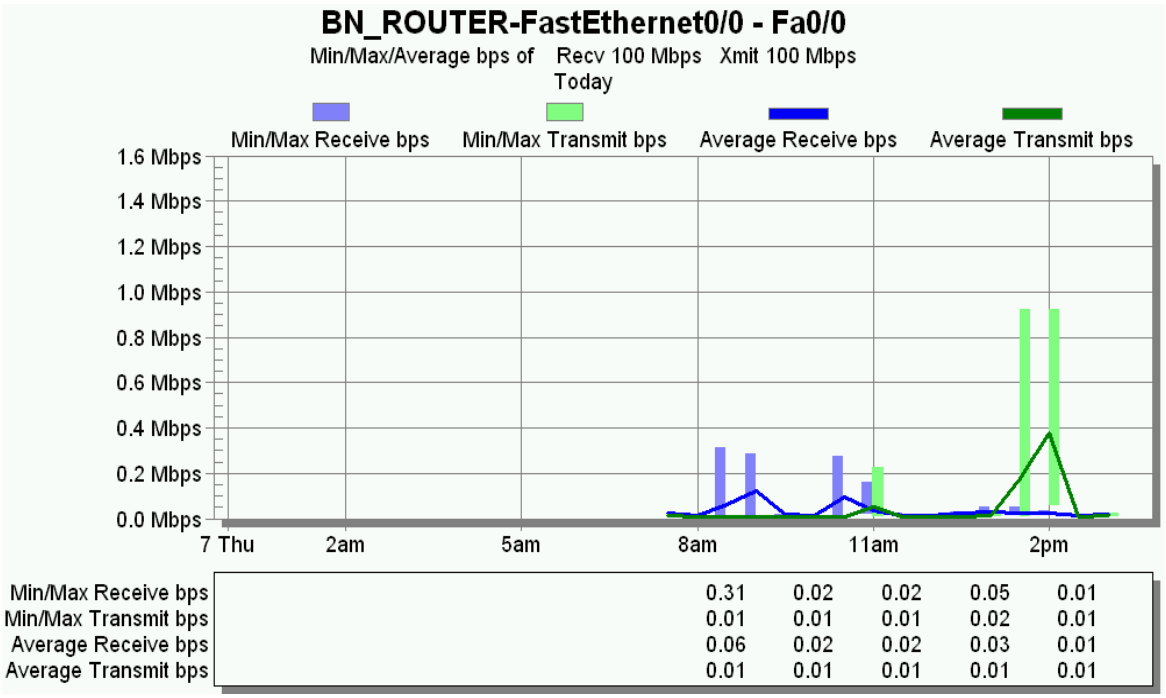

Figure 56. Battalion Router Fast Ethernet Interface 0/0 Performance.

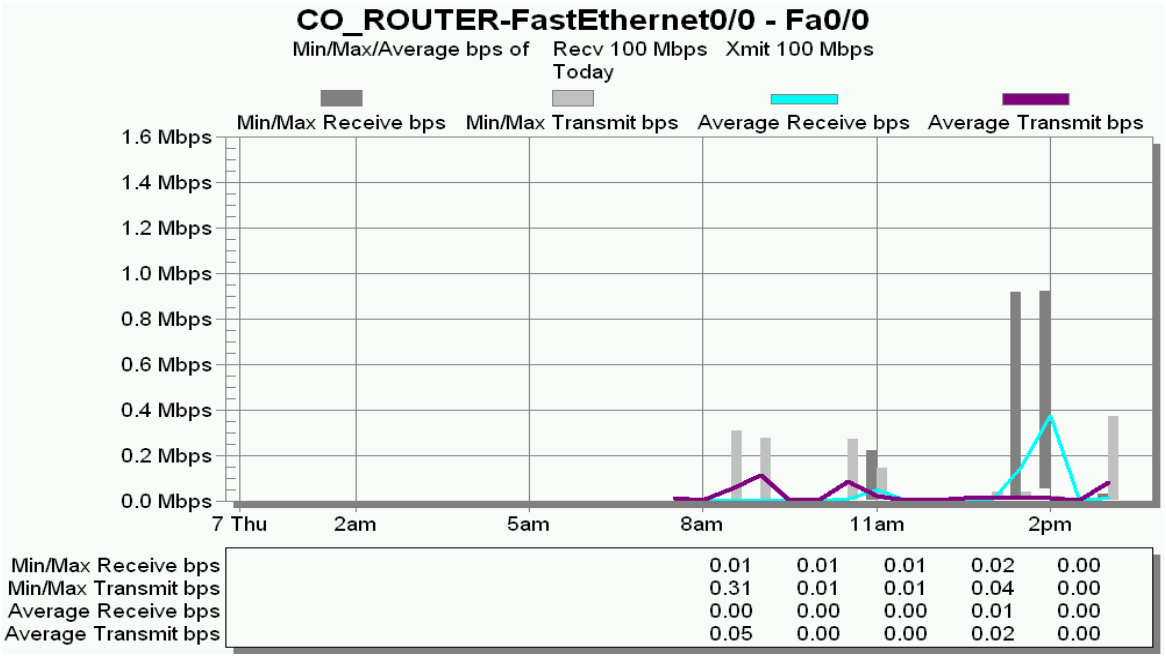

Figure 57. Company Router Fast Ethernet Interface 0/0 Performance.

It is also relevant to note the performance of the Fast Ethernet interface 0/1 (Fa 0/1). It serves as the connection from the router to the layer 2 network switch located at each node. Figures 58 and 59 illustrate the performance of the Fa 0/1 interfaces on the Battalion and Company routers, respectively. The performance of each of the interfaces is consistent with each other. There was no information that would indicate loss of packets between the router and the switch at each node.

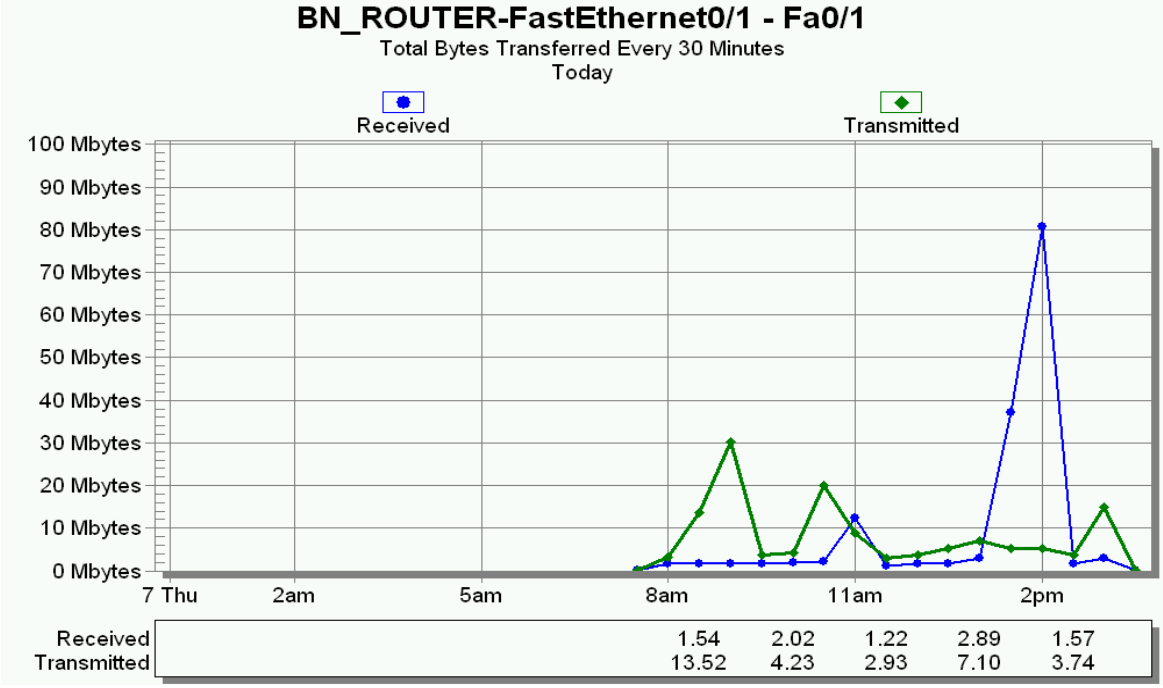

Figure 58. Battalion Router Fast Ethernet Interface 0/1 Performance.

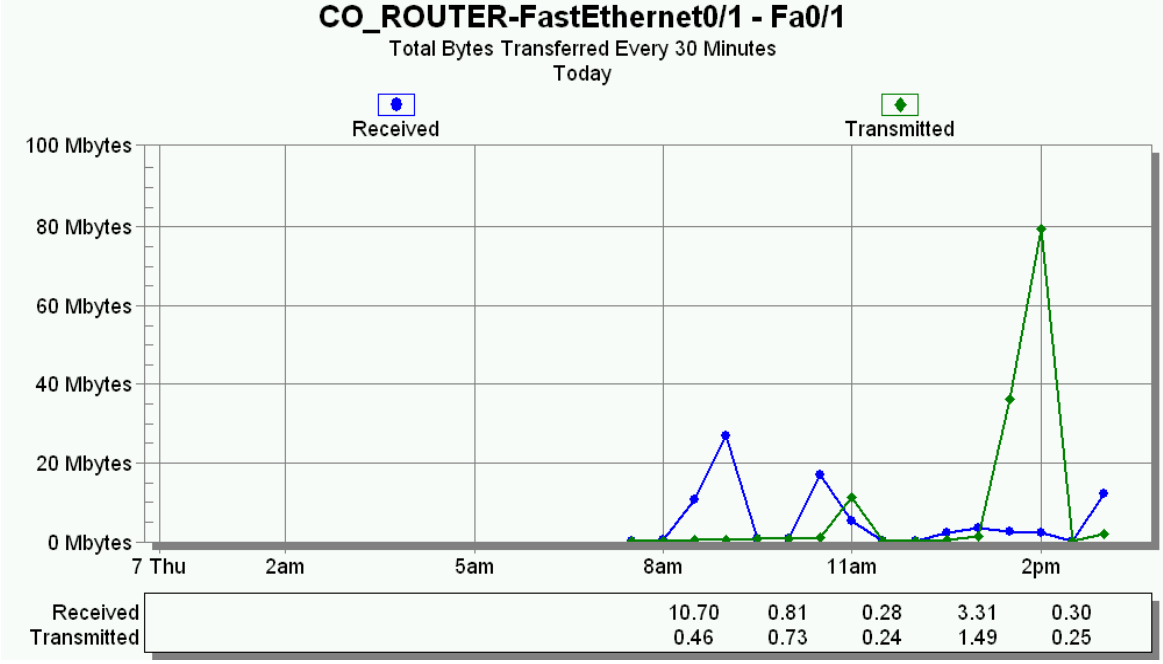

Figure 59. Battalion Router Fast Ethernet Interface 0/1 Performance.

In addition to the network routers, the performance of the network switches was also relevant. As mentioned with regard to the routers, the capability of the deployed switch was beyond that of the transmission system, but, for the purposes of illustrating the ability to perform remote management of network devices, the examination of the switches was germane to the experiment. The important data with regard to the switches was the MIN/MAX response time and packet loss. Figures 60 and 61 illustrate the captured data. The significance of this information is that, as with each of the routers, there is negligible packet loss. The response time of the Battalion switch is consistent with the response time of the respective router. Again, this was because the data collected was done locally. As with the Company router, the response time for the Company switch is consistent with that of the router and with operating on a geostationary satellite link.

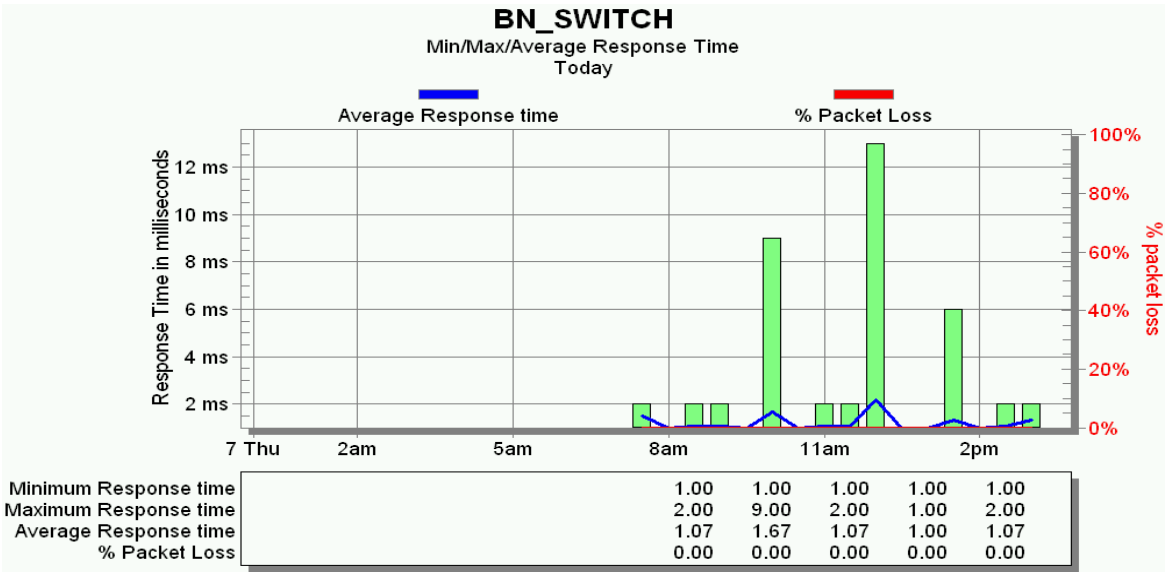

Figure 60. Battalion Switch Response Time and Packet Loss.

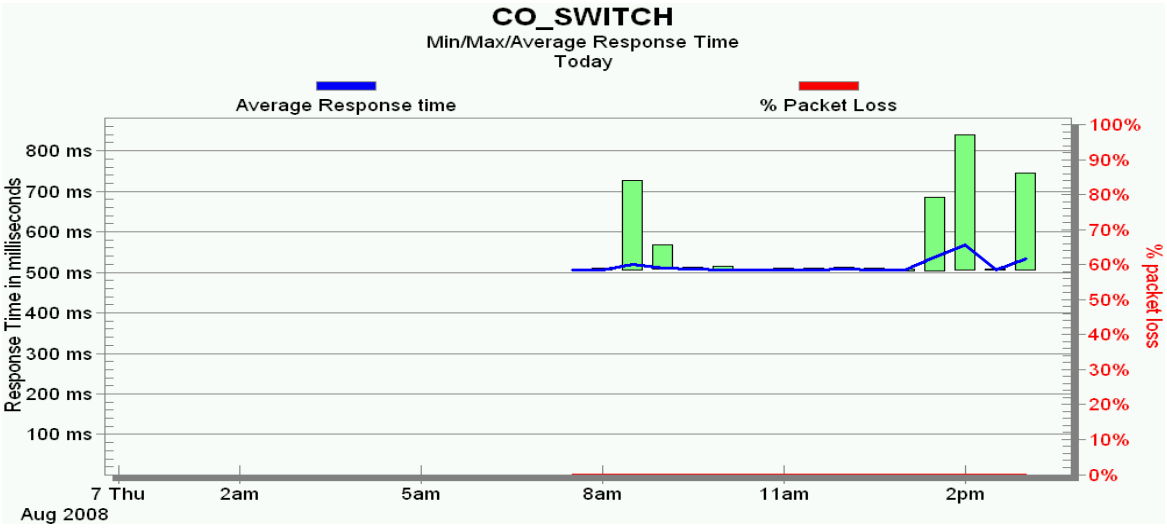

Figure 61. Company Switch Response Time and Packet Loss.

Since the performance of the networking components has been collected and illustrated, the next step in the testing was to utilize common network management protocols to actually conduct management on local devices as well as devices that are

deployed on the distant end of the link. SNMP allows management tools to not only collect data on performance, but also allows the manager to set variables through agents on managed devices in Internet Protocol networks (Hia, Midkiff 190). SolarWinds Engineering Edition allowed the network manager to automatically configure SNMP polling intervals and to automatically poll the devices in question. In the case of this experiment, a polling interval was set at 120 seconds and 240 seconds. Information on device status is relayed back, again using SNMP, to the network management console. The protocol analyzer, WireShark, was used to capture and display the SNMP packets that were transmitted during the experimentation. Figure 62 provides a sample of the SNMP traffic that was transferred during testing:

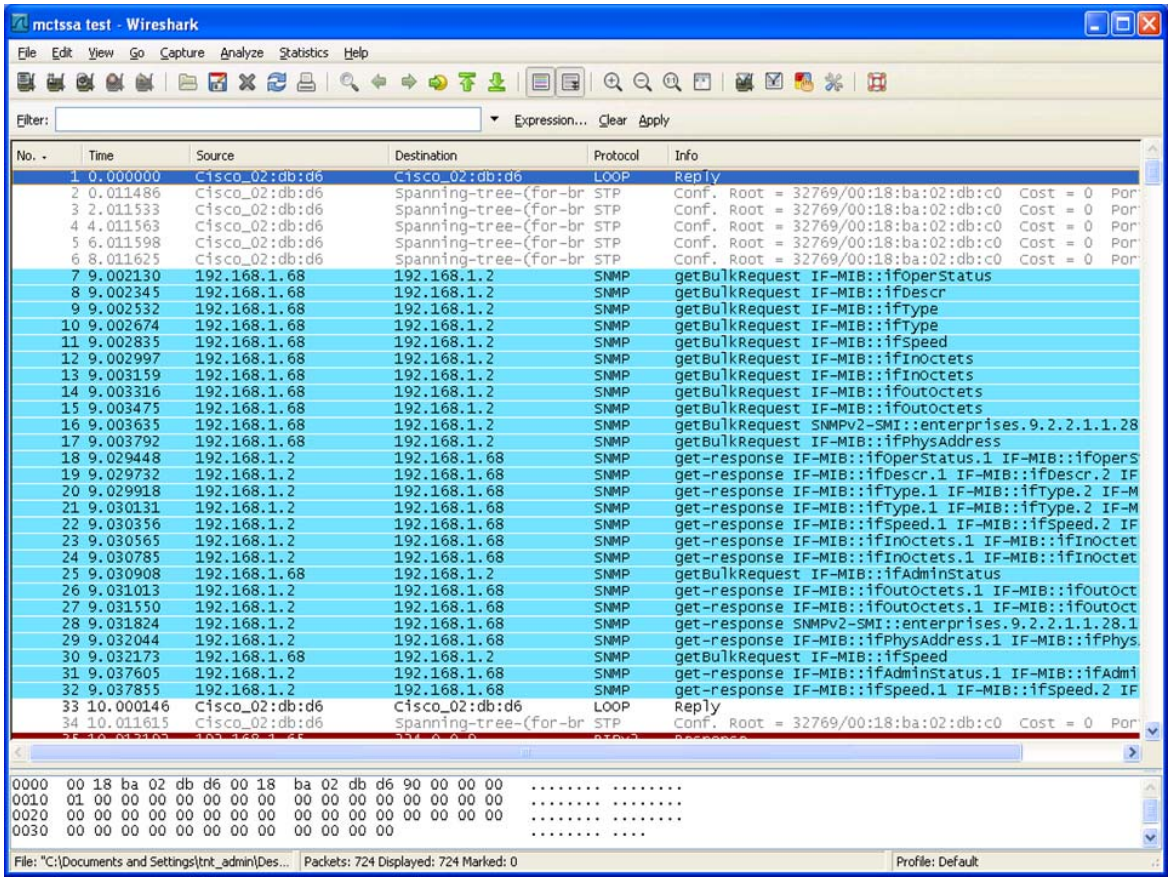

Figure 62. SNMP Sample Data Capture.

It is important to note that SNMP is a recognized standard and is implemented in most commercially available networking devices. There are some cases where the Management Information Base (MIB) is not accessible by automated management tools such as SolarWinds. The iDirect modem in the Swe-Dish IPT is an example of this issue. Access to the MIB for the modem is not permitted by the equipment manufacturer. This is a limitation of the equipment used during the experimentation.

In addition to utilizing SNMP for management, the common ICMP was also utilized for management purposes. ICMP provides simple network discovery and troubleshooting tools that can be used for a variety of management purposes. The common use of ICMP is the PING command. As well as automatically polling for SNMP data, the management software used can automatically send a PING to various nodes on the network. The illustration below (Figure 63) demonstrates the ICMP messaging during the experimentation. As with the SNMP data, WireShark was used to capture and display the packets of interest.

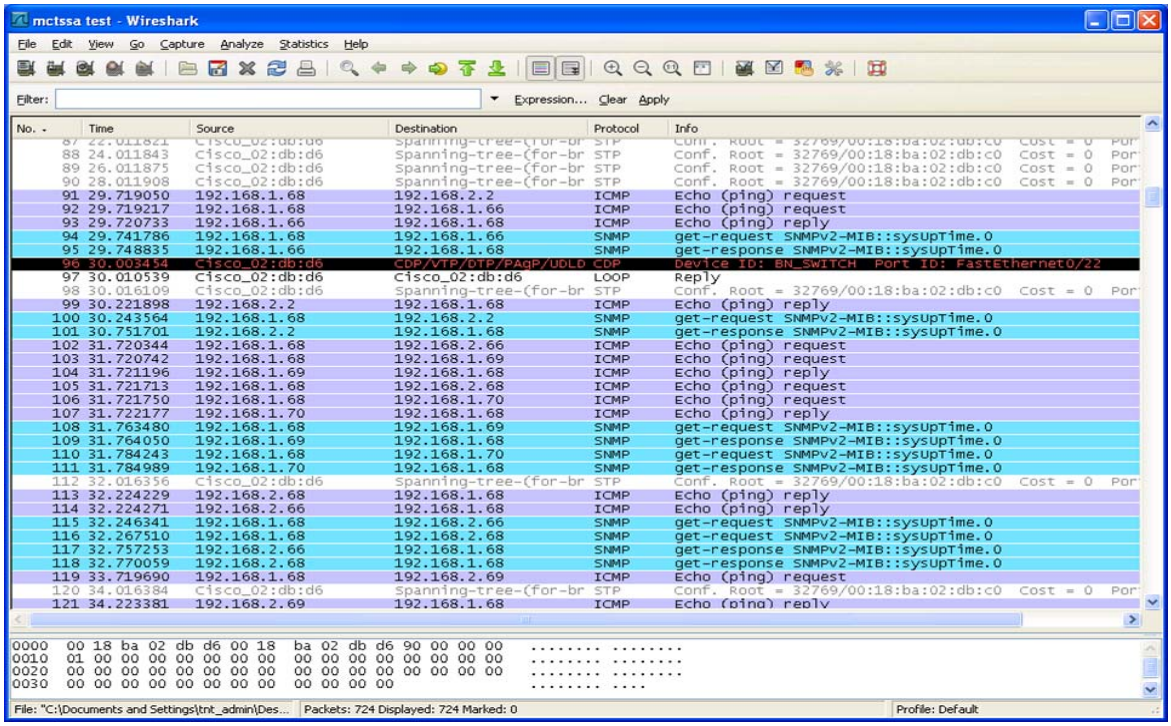

Figure 63. ICMP Sample Data Capture.

4. Conclusions Drawn from the Experimentation

There are several conclusions that can be drawn from the experiment. The first conclusion is that the Swe-Dish IPT, which was the only available resource for the specific experiment, candidate satellite terminals can provide the requisite capability to function as the primary transmission system for the Tactical Private Satellite Network. Considering, however, that a critical factor in the concept of the Tactical Private Satellite Network is a base station/gateway type system, the Swe-Dish IPT is not adequate for that purpose, but could adequately function as the transmission piece for a subordinate node on the network. The performance data collected during this test and during the MIO 08-2 experimentation emphasizes the capability of the Swe-Dish IPT and satellite communications in general. Overall, the satellite link provided by the Swe-Dish and the commercial satellite that bandwidth was provided remained reliable for the duration of the experiment. With regard to the terminal's performance and in terms of the five test samples, there were no significant issues to report. There were significant operational issues associated with the Swe-Dish terminals that were overcome by perseverance on the part of the experimentation team in concert with technical personnel from the equipment manufacturer.

The second conclusion is that during the course of the test and experimentation, the network manager was able to collect network baseline information for both networking devices and the satellite terminals. Although the baseline and performance data is relevant, it is necessary to consider that future testing should incorporate the induction of faults to test detection, isolation, and correction. Relevant data on critical networking devices was also collected track the performance of the devices and any adverse affects that would be introduced into the overall network performance should one of the devices have failed. The data was collected using commercially-available software management tools that use standard management protocols, such as ICMP and SNMP. In addition to the collection of data, the method of collection is critical. During the test, the network manager was able to remotely manage, in a very elemental way, network devices across the satellite link. This was done by using SNMP, ICMP, and TELNET to actively monitor, track, and manage network components. The concept of remote network management is a critical element to the implementation of the Tactical Private Satellite Network.

Third, deployed devices enabled the dissemination of data across the network with no significant loss of data or introduction of any latency other than that naturally occurring due to the characteristics of the geostationary satellite link.

In summary, the test network that was implemented can be perceived as representative of the conceptual Tactical Private Satellite Network. Efforts have been made so as remote network management to be demonstrated through the experimentation at MCTSSA, either as a portion of the bandwidth that can be used to perform management functionality or as the entire satellite link that can be utilized as a network management control channel. There are noted differences, such as there was no base station/gateway device acting as the NECOS for the network and that there were only two nodes established, when in actuality there would be more than two. The ability to utilize satellite communications as the means for information exchange and the capability to remotely manage the network devices and monitor the satellite modem, without owing the space asset, is crucial to operational implementation.

D. APPLICATION OF REMOTE NETWORK MANAGEMENT TO THE TACTICAL PRIVATE SATELLITE NETWORK

The application of remote network management within the context of the Tactical Private Satellite Network requires more detailed analysis. The main management issue regarding the implementation of the Tactical Private Satellite Network is that the management of the satellite link and the management of the networking devices are segregated. Presently, as demonstrated through experimentation, the modems embedded with the satellite terminals are monitored, but not managed, through a proprietary software application. On the other hand, management of the networking components is managed by yet another application. To simplify managerial tasks, the Tactical Private Satellite Network must be viewed as a holistic network where the performance of one aspect, the satellite link and terminal, will directly affect the performance of the other, the networking devices in this example.

With regard to the satellite terminals, there are unique challenges associated with the management of satellite terminals. However, satellite terminals are capable to carry

out multitude tasks, while on the same time a critical mission of the terminal segment is to support end user services (Totsline and Gopal 3). Within the construct of the Tactical Private Satellite Network, the base station/gateway would provide that support to the end-user services. Specific to the management concept is that a common set of management functions must be applied to the satellite terminal portion of the network. These functions include the ability to view and modify satellite network assets (in the case of the Tactical Private Satellite Network, the user terminals), the ability to identify faults within deployed terminals, track overall performance and accounting metrics per terminal, and provide a platform for security management (Totsline and Gopal 3). To achieve this capability within the Tactical Private Satellite Network, a base station/gateway solution, empowered with all the above capabilities, must be employed to address all of the functionality listed.

Another aspect of management is the segregation of communications control/network management data from operational-related C2 data within the aggregated satellite bandwidth. In this case, network management can be achieved through the implementation of a Network Management Control Channel. The idea of the control channel is to logically segregate a portion of the transmission bandwidth. In this case, there is a portion of the satellite link for the purpose of communications control and network management. This control channel could be established within the Tactical Private Satellite Network and utilized to conduct active management on networking components that are a part of the distant stations' local networks utilizing the SNMP. This segregation would minimize the impact on the operational traffic that has to traverse the same channels of the transmission media. Should the creation of a separate channel dedicated to network management not be feasible, means must be addressed to limit the amount of bandwidth required to conduct active network management. In either case, the management protocol performance needs to be balanced against its overhead and the impact of adding network management to managed nodes must be minimal, reflecting a lowest common denominator.

As demonstrated in the experiment, SNMP version 1, ICMP, and TELNET traffic did not have any significant adverse impact on the exchange of data between the two test

nodes. The artificiality, induced by the testing environment, limited the actual number of active nodes on the network to two active nodes. At each of these two nodes, there was one router, one switch, and three hosts. Therefore, it is possible to assume that with a larger network, more bandwidth will be consumed and there will be less available for management functionality. Methods need to be investigated to streamline the network management data and information exchange to not interfere with the transmission of other operationally related data.

To summarize, the ability to remotely manage network resources is critical to the implementation of the Tactical Private Satellite Network. The employment of a base station that has the capability to actively manage various aspects of the deployed satellite terminals would greatly enhance network performance and management. As well, the creation of a network management control channel that rides a subset of the allocated satellite bandwidth with the express purpose of the transfer of network management/communications control information would greatly enhance management efforts — given that there will be no noticeable trade-off with the actual operational channel. Finally, any ways to streamline the flow of management data would greatly improve a remote management capability within the Tactical Private Satellite Network.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY, CONCLUSIONS, AND FUTURE WORK

A. SUMMARY OF WORK

With the growing need for information exchange within the context of military operations and the fact that military operations occur in more dispersed locations, generally where access to the terrestrial telecommunications infrastructure is limited or non-existent, providing broadband routable network access to military units deployed on land, at sea, or to participating heterogeneous units (military and civil authorities), providing humanitarian help in an area that has suffered a major disaster is critical. Since satellite communications is sometimes the only way for deployed units (ships and ground units) to communicate, considering that the MILSATCOM capacity is becoming more saturated, commercial satellite systems and infrastructure have filled the need not covered by either terrestrial systems or MILSATCOM. This has been demonstrated by the fact that the Defense Information Systems Agency has programs in place to contract for commercial satellite services and that an increasing amount of commercial-based satellite terminals are being deployed to military units. The need for a conceptual network that utilizes the commercial space segment, reaches deployed users either on land or at sea, and being managed by its users and not the entity that provides the service has been the focus of this research effort. During the course of research, this effort has covered numerous subjects all related and relevant to the formulation of a conceptual framework for a Tactical Private Satellite Network. This examination was done through an extensive review of relevant literature, the formulation and definition of the conceptual network, the application of this network concept within the context of several scenarios, and testing and experimentation on a live network to demonstrate certain capabilities. To provide an understanding of the concept as described, it was necessary to examine several issues that form the basis for the formulation of this conceptual network.

The first issue examined dealt with the current state of MILSATCOM and the current state of the commercial satellite communications market. Second, a definition of the Tactical Private Satellite Network utilizing primarily the commercial space segment was formulated and a set of capabilities illustrated as to what kind of service this

conceptual network should be able to provide to the user. The most important aspect to the concept of the Tactical Private Satellite Network was to define the central node of the network: a gateway/base station type device that serves to control media access between subordinate terminals, thus, allocating finite satellite bandwidth between member stations of the network, providing the Net Control Station functionality, and serving as a central management agent. Additionally, an examination was conducted into the implementation of the Tactical Private Satellite Network into several use cases: the research environment, a maritime scenario, a scenario associated with the Marine Corps' operational concept of the Security Cooperation Marine Air/Ground Task Force, and within a coalition environment. These scenarios provided additional insight as to the overall utility of this conceptual network for operational and research purposes. Finally, an understanding that the implementation of such a conceptual network within the context of the use cases listed relies upon the ability to conduct remote network management of not only the allocated satellite bandwidth, but also the deployed network devices was illustrated. The ability to conduct remote network management utilizing a portion of the satellite channel is required to deploy such a network and was also demonstrated during the course of the research effort.

As a result, first, it was concluded that if satellite communications are necessary to support military operations across the spectrum of conflict and, if the MILSATCOM constellations are used to maximum capacity, then, commercially available satellite communications services could be and should be leveraged to support military operations. The Department of Defense has recognized that commercial satellite communications services can support military operations in two major ways. First, the Defense Information Systems Agency has procedures and plans in place to acquire commercial satellite communications services for the military. Second, terminal devices that are being fielded to the military that operate on the commercial space segment are proliferating. An example of this would be the U.S. Marine Corps' SWAN program where commercial satellite terminals have been procured and fielded to augment fielded terminals that operate on the MILSATCOM constellation. Therefore, since the capacity on the commercial satellites is available for purchase, the terminals are becoming more

available and the MILSATCOM constellation has little residual capacity. Thus, the commercial space segment is a viable option to support military operations. The use of the commercial segment is an integral part of the conceptual definition and framework for the Tactical Private Satellite Network.

Since it has been determined that commercially-available satellite communications services (access to satellites and bandwidth) is a viable alternative to MILSATCOM and, after the formulation and definition of the Tactical Private Satellite Network, the next step in the research was to look at a live implementation of this conceptual network to demonstrate that the Tactical Private Satellite Network can be implemented and that commercial satellite terminals are usable within the context of the network. The example that was used was taken from the MIO experimentation conducted in March 2008 in and around the San Francisco Bay area. To test the concept, a routable network was established using two commercially-available satellite terminals in a point-to-point configuration to serve as a redundant communications link. Experiment-related traffic consisted of different types of application data. During the course of the experimentation, the primary link failed so all experiment-related traffic was transferred to the satellite link for transmission. The commercial satellite terminals were able to handle the traffic with no degradation in service. This particular case is similar to the provided definition of the Tactical Private Satellite Network in that there was no outside commercial base station providing MAC for the network. The limitation was that there were only two terminals and neither one had the capability to function as the Net Control Station by providing active management of the allocated bandwidth. This was a limitation introduced by the fact that the research entity has only two terminals and no base stations. Even though there were limitations, this live experimentation demonstrated that the Tactical Private Satellite Network could be implemented to support the exchange of information across a commercial satellite link, regardless of the type of application data that must traverse the network. Overall, experimentation inside the framework of MIO 08-2 demonstrated the concept of utilizing the Tactical Private Satellite Network as a method of direct delivery of data.

The concept of remote network management inside the given bandwidth framework from the commercial provider is critical to the implementation of the Tactical Private Satellite Network. Thus, the final conclusion that will be illustrated is the results from experimentation and testing of the concept of remote network management. In August 2008, testing and experimentation was conducted at the Marine Corps Tactical Systems Support Activity in Camp Pendleton, California to investigate this critical concept. The experiment was designed to simulate the transmission of application specific data from one node (functioned as a subordinate headquarters) to another node (functioned as the higher headquarters) via a routable network. Each node had an identical topology with regard to network devices (routers, switches, and hosts) and each node was serviced by a commercial satellite terminal using commercial communications satellite bandwidth in a point-to-point configuration. The point of the experiment was to establish a network management agent at the higher headquarters node and to try and actively manage the satellite terminals and network devices. Through the use of commercially-available network management software, the network management agent was able to actively manage network devices through the satellite link from a central location with little to no degradation in overall service. This remote management used common protocols, such as the SNMP version 1, the ICMP, and TELNET (although not advisable over a satellite link). There were several limitations regarding this experiment. First, there were only two terminals employed: in an operational implementation of a Tactical Private Satellite Network, there would be at least three, and most probably more, with one of the terminals functioning as the Net Control Station with resident gateway functionality. Second, the network was limited to three hosts per subnet; thus, the management responsibilities were scaled back. The third issue is that no encryption was used on the satellite link. The introduction of the encryption, it is assumed, would reduce the amount of throughput on the satellite link. As a result of the experimentation on a live network, it was determined that the current commercial satellite terminals and the associated modems could be monitored only. This was a result of the proprietary nature of the MIB and that the equipment developer would not grant access to the MIB for the purposes of managing the modem embedded in the satellite terminal. With regard to the

deployed network devices, there was no issue in conducting active management remotely. The network manager was able to use TELNET to access the configuration of the routers and switches deployed downstream, as well as the SNMP version 1, to conduct other management functions. Overall, the network manager was able to remotely manage aspects of this experimental routable network. This proven ability to remotely and actively manage satellite terminals and deployed network devices will serve to centralize personnel with network management and engineering skills and provide a management capability for the entire network.

As noted, there were several topics that were examined during the course of this research to lay the foundation for the reader's understanding of the conceptual Tactical Private Satellite Network. In subsequent sections, the conclusions that were drawn from the research will be illustrated and explained, followed by recommendations for future work that were originally outside the original scope of this work.

B. CONCLUSIONS DRAWN FROM RESEARCH EFFORT

The purpose of this research was to propose a framework for managing a tactical network by allocating the available bandwidth to the different users with respect to their needs and the quality of their applications. Commercial leased lines, whose bandwidth is going to be negotiated by the service level agreements between the provider and the consumer (military and governmental agencies), were examined as the means for achieving the connectivity, which was in contrast with the potentially saturated proprietary military satellite communications. The end product will be a tactical network operating inside the overall leased bandwidth's boundaries, but with the capability to manage this network inside them. The term that aggregates these capabilities is the Tactical Private Satellite Network.

The concept of Tactical Private Satellite Network was examined based on two approaches. First, the establishment of two different logical channels inside the physical one was proposed instead of an aggregated channel which serves logically and physically both requirements. By that a portion of the bandwidth is dedicated to the management data which are kept separate from the tactical ones. The proposed segregation needs to be

examined to take under consideration and adjust accordingly the impact on the operational traffic that has to traverse the same channels of the transmission media. Second, the concept of a private satellite network and its implementation was examined as a method for direct delivery of data. This private network will give the notion to its subscribers of security and availability for the provided connectivity. It is further enforced by the execution of network management by one or more base stations which will be operated by the participants and not by the provider of the satellite channels.

The research effort and the formulation and definition of the conceptual Tactical Private Satellite Network lead to three major conclusions. These conclusions are that the use of commercial satellite communications are a viable alternative to MILSATCOM, the concept of this routable Tactical Private Satellite Network can be employed within the context of various use cases (and has been before during experimentation conducted by the CENETIX at the Naval Postgraduate School), and that remote network management over a satellite link is not only feasible, but practical and possible.

To summarize, the conclusions that have been ascertained and demonstrated through the research effort have strengthened the case for the viability of the Tactical Private Satellite Network and its operational implementation. Since the use of commercial terminals and the commercial space segment is a viable alternative to military-only systems, the fact that a representative network was implemented and used successfully to transport live experimental data and the ability for a network manager to conduct active management from a remote location all support the concept of a Tactical Private Satellite Network.

C. SUGGESTED FUTURE WORK

Even though various critical aspects of the Tactical Private Satellite Network have been demonstrated throughout the course of research and, since the Tactical Private Satellite Network has been developed as a concept to this point, there are areas that are suggested for further study within the context of the Tactical Private Satellite Network.

Each of the areas for future research will serve to increase the understanding of the operational implementation of this conceptual network, and broaden the overall utility of the network.

The first aspect for future research deals with the actual implementation of the concepts defined with regard to the base station/gateway device. Since the concept of the Tactical Private Satellite Network requires the employment of a gateway device that will actually provide Media Access Control and modem management for all of the subordinate terminals on the network, the acquisition of such a system would further prove the concepts illustrated in this thesis. The solution may be a physical base station from the same manufacturer of the commercial terminals used by the research team or a modem type device that physically and logically connects to the satellite terminal to provide the functionality described. In addition to the physical solution, the investigation of logical solutions must also occur. This is to say that commercial satellite service providers may have some mechanism to provide a generic terminal connected to their network the capabilities outlined of the gateway/base station device. This device would, then, be able to actively manage all satellite modems and provide MAC for the network.

Another area of future research is continued live testing of the concepts outlined in the body of this work. Continued testing within the experimental environment will serve to clarify concepts outlined, as well as discover new ways to implement not only the satellite terminals, but also implement a routable network using the terminals. The roadmap for such a campaign of experimentation to prove the significance of implementing a Tactical private Satellite Network will have to follow the triad discovery-hypothesis-demonstration (Alberts and Hayes, Code of Best Practice Experimentation, 19-24). At first, thorough discovery experiments need to be conducted to introduce the concept of managing a satellite network provided by a commercial entity. These experiments will be the foundation for more rigorous types of experiments. Then, hypotheses experiments need to recruit that will be subject to more rigorous assessment and refinement so as to build or advance the knowledge on the specific domain. Last, demonstration experiments will be conducted to display that knowledge and the overall necessity of the Tactical Private Satellite Network. These different kinds of experiments

serve to complement and build upon one another and, as the campaign unfolds, our conceptual model of the network will change and hopefully mature over time (Alberts and Hayes, Code of Best Practice: Campaigns of Experimentation, 71).

With the varied testing that is conducted by the CENETIX — especially during the TNT MIO with its adaptive mesh topology and advanced command and control toolsets that could allow for the introduction of such a promising network —, the implementation of the Tactical Private Satellite Network will provide another vector for information and experiment-related data to be disseminated. In addition to implementing this conceptual network within the context of the research environment, it is also important to implement, under the guise of experimentation, the conceptual network in simulated operating environments, similar to the use cases that were outlined previously in Chapter III. Ultimately, this type of implementation will serve to prove whether or not the Tactical Private Satellite Network has any utility within these operational scenarios. Ideally, once all of the requisite hardware has been procured (base station and more terminals), the concept for the Tactical Private Satellite Network should be overlaid on top of operational forces for their ultimate evaluation of the concept and to determine the overall utility. Being that research has been conducted on this subject to this point has reinforced the derived concepts, no actual implementation of the defined Tactical Private Satellite Network can occur until the topology has been solidified and the equipment for implementation has become available.

Within the implementation in the context of the experimental environment, as the level of confidence in the equipment and the concept increases, it is strongly recommended that the level of complexity and sophistication of the test networks increases as well. During experimentation, only limited amounts of representative application data was transmitted over the satellite link. The addition of different types of devices, such as biometric devices, pico-cell technology, the connection of various land mobile radio devices, VPN concentrator, live video feeds, audio, database pulls, and on will all aid in the evaluation of the Tactical Private Satellite Network concept. Also, ascertaining and evaluating the information exchange requirements of operational units

will aid in the determination of what application data actually needs to be passed over the satellite link. This will be based on priorities set by the operational unit.

One area of complexity that crosses boundaries of operation and management of the Tactical Private Satellite Network and requires future research is the implementation and testing of this concept in a coalition environment. Coalition environments can be established in response to domestic natural disaster response (such as between the military and civil authorities) to those coalitions built to address a threat to collective security, such as the coalitions that have been built to support operations in Iraq. There are technical and managerial issues that are complex, but political issues could potentially exacerbate the pre-existing technical problems as well. Therefore, network operations and management within the context of the coalition environment is worthy of further study — not only within the context of the Tactical Private Satellite Network, but in general. The theoretical implementation of the Tactical Private Satellite Network, being technologically agnostic, into the coalition environment could have great benefit within this scenario.

By not only having varied amounts of traffic traverse the network, it is just as critical to continually examine technologies, tactics, techniques, concepts, and procedures that deal directly with the management of this conceptual network. As mentioned previously, the basic ability to conduct active remote network management has been demonstrated, but further steps need to be taken. The experimentation in remote network management that was conducted was limited in scope. Further research in the area of remote management would be to introduce faults into the network, to evaluate the ability of management tools and personnel to identify and handle the faults, and to identify ways to increase overall network availability.

Another very important area of suggested study within the realm of the Tactical Private Satellite Network is security. The live experimentation that was conducted focused primarily on the basic concepts required for the fundamental operation of the network. Because commercial satellite services used to transmit data had no classification associated with it, security requirements were considered, but not tested. Within the context of security, there are three areas that could be addressed either individually or

collectively. The first area is physical security. Physical security, in this instance, is not limited to making sure that the satellite terminal is not compromised (stolen, damaged, etc.), but securing the Physical (reference Layer 1 of the OSI model) Layer. This is done by implementing MAC. The concept of the Tactical Private Satellite Network calls for the employment of a base station device that would provide Media Access Control for the terminals on the network. Since the research team did not have access to such a device, that concept could not be demonstrated. It is suggested that the base station device would protect access to the media that was procured to support specific customers for a specific mission. Further study of this would require the acquisition of the base station and its employment in a use case. The second issue relating to security is addressing the Information Assurance triad of Confidentiality, Integrity, and Availability. There are various ways in which this can be examined within the context of the Tactical Private Satellite Network and it is recommended that this occur because operational traffic that traverses this conceptual network is worthy of protection. The final issue for consideration for future work is the use of the SNMP version 3 which provides for secure network management. Remote network management has been demonstrated with version 1 of the SNMP, but, to provide a more secure management environment, the implementation of SNMP version 3 is required.

Another possible area of investigation could be the implementation of the NECOS, and other critical nodes of advanced capabilities, as hyper nodes of the 8th layer which, with their own specialized NOC capability, could implement adaptive networking. These hyper-nodes could demonstrate capabilities, such as self-diagnosis, sub network view, end-to-end performance, QoS requirements response, and Service Level Agreements negotiation (Bordetsky and Hayes-Roth). The result of such a proper implementation could be the relieving of rigorous management for the central network station and, consequently, the creation of a more flexible model of efficient management of such an ad hoc dynamically-formed network and the releasing of additional bandwidth for strictly operational needs.

To summarize, there are numerous areas for future study that build upon the concept of the commercial satellite-based Tactical Private Satellite Network with the

ability to be managed by its users. Areas of future implementation, within the context of an experimental research environment, a simulated operational environment, as well as a real operational environment, to include coalitions, are all candidates for future work. Additionally, the security aspects of the Tactical Private Satellite Network need to be addressed before any operational implementation can be considered.

In any case, further research should be conducted to examine more thoroughly the functionality and feasibility of the Tactical Private Satellite Network in laboratory and real situation conditions. From the whole research, networks formed under adverse and dynamic conditions, such as the case of Tactical Private Satellite Network, will provide great benefit because their network management will become more efficient, complete, and robust to guarantee safe and continuous communication lines during life-significant missions.

THIS PAGE INTENTIONALLY LEFT BLANK

WORKS CITED

"Active FTP." Cross FTP Knowledgebase. 09 August 2007. Cross FTP Knowledgebase. 27 August 2008. http://www.crossftp.com/kb/entry/20/.

Alberts, David S., Garstka, John J., Stein, Frederick P., Network Centric Warfare. Department of Defense C4ISR Cooperative Research Program. Washington, D.C. 1999.

Alberts, David S et al. Understanding Information Age Warfare. Department of Defense C4ISR Cooperative Research Program. Washington, D.C. 2001.

Alberts, David S and Hayes, Richard E. Code of Best Practice Experimentation. Department of Defense C4ISR Cooperative Research Program. Washington, D.C. 2002.

Alberts, David S and Hayes, Richard E. Power to the Edge. Department of Defense C4ISR Cooperative Research Program. Washington, D.C. 2003.

Alberts, David S and Hayes, Richard E. Code of Best Practice: Campaigns of Experimentation. Department of Defense C4ISR Cooperative Research Program. Washington, D.C. 2005.

Arvidsson, A, S.A. Berezner, and A.E. Krzesinski. "The Design and Management of ATM Virtual Path Connections." IEEE Explore. Naval Postgraduate School Lib., Monterey, CA. 30 June 2008. http://ieeexplore.ieee.org.

Barabasi, Albert-Laszlo. Linked. How Everything Is Connected to Everything Else and What it Means for Business, Science, and Everyday Life. New York: Plume, 2003.

Bordetsky, A. and Bourakov, E. Network on Target: Remotely Configured Adaptive Tactical Networks. The State of the Art and the State of the Practice. 2006 CCRTS.

Bordetsky, A. and Hayes-Roth, Frederick. Hyper-Nodes for Emerging Command and Control Networks: The 8th Layer. Department of Defense C4ISR Cooperative Research Program, 11th Command and Control Research and Technology Symposium. Washington, D.C.

Buddenberg, Rex. Course Notes. web.nps.navy.mil/~budden/book/two.avail_.html. 15 June 2008.

Burke, Arleigh A. "Use of Satellites for Naval Purposes." OP-OO Memo 00471-59. 26 August 1959.

Celik, E., "A Ground Station Control Software Application." International Conference on Recent Advances in Space Technologies, 2003. November 2003. (177-181, 20-22).

Chambers, Howard. Trends in the Commercial Satellite Industry. Euroconsult 2007. France. Boeing.com. 05 September 2007. http://www.boeing.com/news/speeches/2007/chambers_070905.html.

Chadran, Ram S. "State of California Emergency Response Network." Disaster Resource Guide: Satellite Strategies for Disaster Recovery and Business Continuity. First Quarter, 2007. http://www.disaster-resource.com/articles/SatelliteIssue_Final_HighRes.pdf.

Chotikapong, Yotsapak, Haitham Cruickshank, and Zhili Sun. "Evaluation of TCP and Internet Traffic via Low Earth Orbit Satellites." IEEE Personal Communications Magazine. 2001. (28-34).

Cisco Systems. Asynchronous Transfer Mode. Internetworking Technologies Handbook. http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html. 4 June 2008.

Colella, Nicholas. J., James Martin, and Ian F. Akyildiz. "The HALO network." IEEE Communications. 38 (2000).

Elfers, Glen, Stephen B. Miller. "Future U.S. Military Satellite Communications Systems." Aero.org 2001. 10 May 2008. http://www.aero.org/publications/crosslink/ winter2002/08.html.

Eklund, Carl, Roger B. Marks, Kenneth L. Stanwood, and Stanley Wang. IEEE Standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access." IEEE Communications Magazine. June 2002: 98-107.

Gordon, Gary and Walter Morgan. Principles of Communications Satellites. New York: John Wiley and Sons, 1993.

Harris, Shon. CISSP Exam Guide, Third Edition. New York: McGraw-Hill/Osborne, 2005.

Hart, David. www.cis.ohio-state.edu/~jan/cis 788-97/satellite.nets/index.html. 3 June 2008.

Hia, H. Erik, and Scott F. Midkiff. "Securing SNMP Across Backbone Networks." IEEE Explore. Naval Postgraduate School Lib., Monterey, CA. 31 July 2008. http://ieeexplore.ieee.org.

Hoeber, Chris. Naval Postgraduate School Space Systems Seminar. 2000.

Hook Jr., Jack A. Military Dependence on Commercial Satellite Communications Systems - Strength Or Vulnerability. U.S. Air Force, Air Command and Staff College, Air University. April 1999. DTIC Online. Naval Postgraduate School Lib., Monterey, CA. 31 October 2001. http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD= ADA395141&Location=U2&doc=GetTRDoc.pdf.

"HughesNet Access Continuity Brings Roundtree Automotive's IT Staff Piece of Mind." Disaster Resource Guide: Satellite Strategies for Disaster Recovery and Business Continuity. First Quarter, 2007. http://www.disaster-resource.com/articles/SatelliteIssue_ Final_HighRes.pdf.

Hutchens III, Robert E. DOD use of Commercial Wideband Satellite Communications Systems: How Much is Needed, and How Do We Get it? U.S. Air Force, Air Command and Staff College, Air University. April 2001. DTIC Online. Naval Postgraduate School Lib., Monterey, CA. 20 November 2002. http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA407005&Location=U2&doc=GetTRDoc.pdf.

Internet Engineering Task Force. "Request for Comments." Internet Engineering Task Force. July 2008. http://www.ietf.org/rfc/html.

Iida, Takashi, et al. Satellite Communications in the 21st Century: Trends and Technologies. Reston, VA: American Institute of Aeronautics and Astronautics, 2003.

Institute of Electrical and Electronics Engineers, Inc. IEEE Std 521-2002. New York. 2003.

Jamalipour, Abbas. "Broadband Satellite Networks – the Global IT Bridge." IEEE. 2001 (88-104). Proceedings of the IEEE. Vol 89, No 1. January 2001.

Karaliopoulos, Merkourios, Rahim Tafazolli, and Barry G. Evans. Providing Differentiated Service to TCP Flows Over Bandwidth on Demand Geostationary Satellite Networks. IEEE Journal on Selected Areas in Communications. Vol 22, No 2. February 2004. (333-347).

Kuehne, Tim. TCP/IP Over ATM via Satellite Links. Masters Thesis. University of Colorado at Colorado Springs, 1998.

Lawlor, Marryan. "Marines Build Transformational Bridge." Signal On Line. April 2004. http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=86&zoneid=35.

Mattock, Michael G. Optimal Commercial Satellite Leasing Strategies. Santa Monica: Rand, 2002.

McKinney, Maurice M. Transformational Satellite (TSAT) Communications Systems. Falling Short on Delivering Advanced Capabilities and Bandwidth to Ground-Based Users. U.S. Air Force, Air Command and Staff College, Air University. July 2007. DTIC Online. Naval Postgraduate School Lib., Monterey, CA. 31 October 2007. http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471938 &Location= U2& doc=GetTRDoc.pdf.

Merriam – Webster's Collegiate Dictionary. Eleventh edition. Springfield, Massachusetts. 2003.

Mohney, Doug. "Soaring Condor Relieves Headaches." Mobile Radio Technology, June 2004. http://mrtmag.com/mag/radio_soaring_condor_relieves/index.html.

Monterey, CA. 31 October 2001. http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA395141&Location=U2&doc=GetTRDoc.pdf.

DeMello, Bruce R. Defining Commercial Space's Place in the Battlespace. United States Navy, Naval Command and Staff College. May 2004. DTIC Online. Naval Postgraduate School Lib., Monterey, CA. 19 Jun 2008. http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA426002&Location=U2&doc=GetTRDoc.pdf.

"NetMeeting 3.0 Resource Kit." Microsoft TechNet. Microsoft Corporation. 24 August 2008. http://technet.microsoft.com/en-us/library/cc767134.aspx.

Oikarinen, J., D. Reed. "Internet Relay Chat." Network Working Group, Request For Comment 1459. May 1993.

Olechma, E, P. Feighery, and S. Hryckiewicz. "Virtual Private Network Issues Using Satellite Based Networks." IEEE Explore. July 2008. Naval Postgraduate School Lib., Monterey, CA. http://ieeexplore.ieee.org/iel5/7739/21248/00985945.pdf?tp=&isnumber=&arnumber=985945.

Parikh, Salil, and Robert C. Durst. "Disruption Tolerant Network for CONDOR." IEEE Explore. July 2008. Naval Postgraduate School Lib., Monterey, CA. http://ieeexplore.ieee.org/iel5/10687/33743/01605705.pdf?arnumber=1605705.

Parikh, Salil and Robert C. Durst. "Disruption Tolerant Networking For Marine Corps Condor." IEEE Explore. July 2008. Naval Postgraduate School Lib., Monterey, CA. http://ieeexplore.ieee.org/iel5/10687/33743/01605705.pdf?arnumber=1605705.

Rayermann, Patrick. "Exploiting Commercial SATCOM: A Better Way." Parameters 33.4 (2003/2004): 54-66.

Real-Time Satellite Tracking. 31 July 2008. N2YO. 31 July 2008. http://www.n2yo.com/?s=26056.

Real-Time Satellite Tracking. 05 August 2008. N2YO. 07 August 2008. http://www.n2yo.com/?s=25922.

Satellite Fact Sheet; Galaxy 10R. 31 July 2008. The Satellite Encyclopedia. 31 July 2008. http://www.tbs-satellite.com/tse/online/sat_galaxy_10r.html.

Somji, Faiz. "Satellite Communication and Disaster Recovery." Presentation to United Nations Economic and Social Commission for Asia and the Pacific. June 2005.

Staff, National Plans Branch, Strategy and Plans Division, Plans, Policies, and Operations Department, Headquarters U.S. Marine Corps. "Fighting the Long War." Marine Corps Association.com. The Marine Corps Association. 31 July 2008. http://www.marine-corps-association.com/gazette/jun08_fighting_the_long_war.asp.

Stuart, James R. "Satellite Communication Technologies and Trends." Technology Review and Update. Naval Postgraduate School. Monterey, CA. April 2005.

Tarr, Julie, and Tony DeSimone. "Defining the GIG Core." Military Communications Conference 2007. Institute of Electrical and Electronics Engineers, Inc. 2 June 2008. http://ieeexplore.ieee.org/servlet/opac?punumber=4454732.

Totsline, Greg, and Rajeev Gopal. “On Managing Intelligent Satellite Networks – An Evolutionary Approach in Policy Based Distributed Management.” NavalPostgraduate School Lib., Monterey, CA. 31 July 2008. http://ieeexplore.ieee.org.

United States. Department of Defense. Commercial Satellite Communications (COMMSATCOM) Service Spend Analysis and Strategy Report. Washington, D.C. 2006.

United States. Department of Defense. Defense Commercial Communications Satellite Services Procurement Process. Washington, D.C. 2005.

United States. Department of Defense. Joint Publication 3-14 Joint Doctrine for Space Operations. Washington, D.C. 2002.

United States. Department of Defense. Joint Publication 6-0 Joint Communication System. Washington, D.C. 2006.

United States. Government Accounting Office. Satellite Communications Strategic Approach Needed for DoD’s Procurement of Commercial Satellite Bandwidth. Washington, D.C. 2003.

United States. Headquarters, U.S. Marine Corps. The Long War; A Marine Corps Operational Concept To Meet An Uncertain Security Environment. Washington, D.C. January 2008.

United States. Headquarters, U.S. Marine Corps. USMC SWAN-D CONOPS. February 2008.

United States. Marine Corps Systems Command. System Communications Description for Secure Mobile Anti-jam Reliable Tactical Terminal. Quantico, VA. 2007.

United States. Naval Postgraduate School. Networking and Collaboration on Interdicting Multiple Small Craft Possessing Nuclear Radiation Threat. Monterey, California. March 2008.

United States. U.S. Special Operations Command. USSOCOM Mobile SSEP Preliminary Design Review. May 2008.

Wikipedia. http://en.wikipedia.org/wiki/2004_Indian_Ocean_earthquake. 29 July 2008.

Wilson, Jim D. “MCSC CONDOR Information Brief.” U.S. Marine Corps, Marine Corps Systems Command. January 2005. https://www.mccdc.usmc.mil/OpsDiv/CEAB/Jan%2005%20CEAB/CONDOR.ppt.

Zeber, S., J. Spagnolo, and D. Cayer. “The Dynamic VPN Controller: Secure Information Sharing in a Coalition Environment.” Technical Memorandum, Defense Research and Development Canada. March 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California